



Interested in learning more
about securing Oracle?

SANS Institute

Security Consensus Operational Readiness Evaluation

This checklist is from the SCORE Checklist Project. Reposting is not permitted without express, written permission.

Oracle Database Security Checklist

Oracle Database Checklist

Prepared by Pete Finnigan

References:

Oracle security step-by-step – A survival guide for Oracle security – Pete Finnigan - SANS Press – April 2004 (version 1.0 and version 2.0)

Links to many useful papers and presentations about Oracle security – <http://www.petefinnigan.com/orasec.htm>

Oracle security website <http://otn.oracle.com/deploy/security>

Oracle Corporation main page <http://www.oracle.com>

Customer support site <http://metalink.oracle.com>

Security alerts <http://otn.oracle.com/deploy/security/alerts.htm>

Introduction:

This checklist is to be used to audit an Oracle database installation. This checklist is just that “a checklist” and does not contain any specific SQL or shell commands because it is intended to be just a list rather than a “how to” document otherwise. It is also important that the Oracle database is not checked in isolation and the surrounding elements such as the operating system used, the network configuration, web access, application servers and clients are considered.

Whilst every effort has been made to ensure that this checklist is as complete and comprehensive as possible new issues and vulnerabilities are found every day therefore don't rely on it to be all encompassing. Regularly check for updates of this list.

Elements to be considered prior to applying this checklist:

- *Host Operating System* – Although this checklist includes items that specifically relate to the operating system hosting the Oracle installation they are included because they have a direct effect on Oracle. It is imperative that the host operating system is secured before any applications (in this case Oracle). The same applies to network components and other applications hosted on the same servers. Please consult other *S.C.O.R.E* documents (<http://www.sans.org/score>), *center for internet security (CIS)* benchmarks and tools (<http://cisecurity.org>) and *SANS* step-by-step guides (<http://sore.sans.org>) for more information.
- *Procedural* – It is important to also consider physical security of the servers hosting the Oracle database and also to employ security procedures and policies and to develop standards for change and control.
- *Findings and data sensitivity* – Establish the sensitivity of the data stored within the Oracle database and establish *rules* for reporting any security findings back to the organisation. This should take into account availability, confidentiality and the integrity of the data. This is important to be able to place any findings within the correct context when reporting back results of an audit.

- *Practicality of the checklist* – This list is the culmination of the knowledge of many Oracle database security practitioners and as such includes every issue thought to be relevant to *somebody*. To some organisations some items are important to be fixed and to others not relevant because of mitigating circumstances. Oracle can be configured in many differing ways and this affects how it is secured. The list has been provided with severity levels to allow the audit to be conducted to a specified level and also includes OS and Oracle versions relevancies.
- *Oracle database security standards* - This checklist could also be used to define a company standard for securing Oracle.

Before using this checklist to review an Oracle database installation it is important to understand the use to which the Oracle database and applications will be put. How the database is used can have a direct effect on how this list is read and interpreted. Oracle is a complicated beast to configure in any multitude of guises and checks and solutions that are relevant for one installation and type of application will conflict with another. Practicality is called for!

Checklist:

Before presenting the checklist a few words about what the columns mean. The *action* column indicates broad sections that checks are grouped into and also includes the action references indicated in the Oracle security step-by-step guide. The severity levels are set between 1 and 5 (1 indicating the highest level). These levels were reached by consensus during the writing of the *step-by-step*. The *O/S* column identifies whether *Unix* or *Windows* or both can be checked. The *Oracle version* column indicates the relevant Oracle installation and finally the *default install* column indicates whether the issue can be considered after a default installation. For ease of identification all of the highest severity issues are indicated by being greyed out.

Action	Description	Severity Level	O/S	Oracle Version	Default Install
0.	Planning and Risk assessment				
0.1	Identify and patch known and reported Vulnerabilities	1	ALL	ALL	YES
0.2	Identify and record software (Oracle and OS and Applications) versions and patch levels on the System	1	ALL	ALL	YES
0.3	Install only the database features that are needed	1	ALL	ALL	YES
0.4	Record database configuration and store securely	2	ALL	ALL	YES
0.5	Record database security configuration and store securely	2	ALL	ALL	YES
0.6	Review database security procedures and policies	2	ALL	ALL	YES
0.7	Store copies of the media used to build Oracle database off site	3	ALL	ALL	YES
0.8	Consider physical location of servers	2	ALL	ALL	YES
0.9	Define secure database / application architecture	3	ALL	ALL	YES
1.	Host Operating System security Issues				
1.1.1	Check owner of Oracle software owns all files in \$ORACLE_HOME/bin	1	ALL	ALL	YES
1.1.2	Lock Oracle software owner account	1	ALL	ALL	YES
1.1.3	Do not name Oracle software owner account <i>oracle</i>	2	ALL	ALL	YES
1.1.4	Limit access to software owner account	2	Unix	ALL	YES
1.1.5	Use separate owners for different components of Oracle such as <i>listener, intelligent agent and database.</i>	2	ALL	ALL	YES
1.2.1	Check file permissions in \$ORACLE_HOME/bin	1	Unix	ALL	YES
1.2.2	Check <i>umask</i> value	1	Unix	ALL	YES

1.2.3	Check owner and group for all files in \$ORACLE_HOME	1	Unix	ALL	YES
1.2.4	Set file system type, user name, group name and file permission issues for Windows	1	Win	ALL	YES
1.2.5	Location of temp directories pointed at by TMP_DIR and TMPDIR	1	Unix	ALL	YES
1.2.6	Check windows groups used for ORACLE_HOME and ORACLE_BASE	1	Win	ALL	YES
1.3.1	Review membership of OSDBA	1	ALL	ALL	YES
1.3.2	Ensure Oracle is not in root group	1	Unix	ALL	YES
1.3.3	Don't use the name <i>dba</i> for the OSDBA group	1	Unix	ALL	YES
1.3.4	Don't use the name ORA_DBA for the OSDBA group on Windows	2	Win	ALL	YES
1.4.1	Check trace file permissions	3	ALL	ALL	
1.4.2	Remove <i>tkprof</i> from production database	3	ALL	ALL	YES
1.4.3	Remove the <i>otrace</i> utility	2	ALL	ALL	YES
1.4.4	Check permissions of the datafiles	1	ALL	ALL	YES
1.4.5	Monitor Oracle log files	3	ALL	ALL	
1.4.6	Check for sensitive temporary files	2	ALL	ALL	
1.4.7	Check for tertiary trace files	2	ALL	ALL	
1.4.8	Check for remote data access files (RDA)	3	ALL	ALL	
1.4.9	Raw device permissions	1	Unix	ALL	YES
1.5.1	Usernames and passwords in process list	1	Unix	ALL	
1.5.2	Restrict the <i>ps</i> command	2	Unix	ALL	YES
1.5.3	Search shell history files for usernames and passwords	2	Unix	ALL	
1.6.1	Secure network transmissions	3	ALL	ALL	
1.6.2	Encrypt data transmissions	3	ALL	ALL	
1.6.3	Secure password transmission on the server	1	ALL	ALL	YES
1.6.4	Secure password transmission on the client	1	ALL	ALL	YES
1.6.5	JDBC thin driver transmissions – ensure minimum permissions of connections used	1	ALL	ALL	YES
1.7.1	Permissions on Oracle SUID and SGID files	3	Unix	ALL	YES
1.7.2	Check for non Oracle SUID and SGID files in \$ORACLE_HOME	3	Unix	ALL	
1.8.1	Audit environment variables for usernames and password	3	ALL	ALL	
1.8.2	Audit the machine for scripts containing usernames and passwords	2	ALL	ALL	
1.8.3	Audit <i>cron</i> for usernames and passwords	2	Unix	ALL	
1.8.4	Audit client machines for configuration files containing usernames and passwords	2	ALL	ALL	
1.8.5	Remove database creation scripts	2	ALL	ALL	YES
1.9.1	Utilize O/S auditing facilities	2	ALL	ALL	YES
1.9.2	Save log files to a separate server using <i>Syslog</i> or Windows event viewer	2	ALL	ALL	YES
1.9.3	Integrity check O/S files used by Oracle	2	Unix	ALL	YES
1.9.4	Consider using host based IDS	3	ALL	ALL	
1.9.5	Review expected processes regularly	2	ALL	ALL	
1.10.1	Check control file permissions	2	ALL	ALL	YES
1.11.1	Confirm who is creating trace files	3	ALL	ALL	
1.11.2	Audit trace files for attempts to read database internal structures	3	ALL	ALL	
1.11.3	Ensure no user has ALTER SESSION and ALTER SYSTEM privileges	1	ALL	ALL	YES
1.12.1	Audit for export file existence	1	ALL	ALL	
1.12.2	Changing database passwords after full import	1	ALL	ALL	
1.13.1	Locate archive log files and check no user except software owner can read them	2	ALL	ALL	
1.13.2	Save archive log files to disk and purge	2	ALL	ALL	
1.14.1	Audit external tables used	2	ALL	>= 9i	
1.15.1	Restrict access to native PL/SQL compilation	1	ALL	>= 9i	YES
1.16	Be aware of key files containing hashes or passwords or other sensitive information	3	ALL	ALL	YES

1.17.1	Password protected listener can be shut down	3	Win	ALL	
2.	Oracle Authentication				
2.1.1	Audit database users activities	3	ALL	ALL	
2.1.2	Audit application database logins	3	ALL	ALL	
2.1.3	Audit users database passwords	2	ALL	>= 8	YES
2.1.4	Establish a policy that prevents users from sharing account ID's	2	ALL	ALL	
2.1.5	Use proxy authentication to help resolve SSO issues	3	ALL	>= 8	
2.2.1	Audit default database accounts	1	ALL	ALL	YES
2.2.2	Add password management for default accounts	1	ALL	ALL	YES
2.2.3	Audit <i>internal</i> alias login	2	ALL	>= 8i	YES
2.2.4	Audit non database Oracle passwords	2	ALL	ALL	YES
2.2.5	Change <i>sys</i> password	1	ALL	ALL	YES
2.2.6	Change <i>system</i> password	1	ALL	ALL	YES
2.2.7	Create business process to audit default accounts regularly	2	ALL	ALL	
2.2.8	Disable remote login password file	2	ALL	ALL	YES
2.2.9	Check use of <i>system</i> tablespace as default	3	ALL	ALL	YES
2.2.10	Modify Oracle scripts for default accounts that are used	1	ALL	ALL	YES
2.2.11	Audit known default role passwords	1	ALL	ALL	YES
2.3.1	Audit users accounts for passwords same as username	2	ALL	ALL	
2.3.2	Audit users accounts for weak passwords	2	ALL	ALL	
2.3.3	Lock dormant database accounts and remove after time delay	3	ALL	ALL	
2.3.4	Stop personal data exposure on users accounts	5	ALL	ALL	
2.3.5	Use obfuscated naming convention for users accounts	5	ALL	ALL	
2.3.6	Use LDAP for external authentication	4	ALL	>= 9i	
2.3.7	Review database accounts, ensuring they belong to business users.	2	ALL	ALL	
2.4.1	Secure remote password login file	3	ALL	ALL	YES
2.5.1	Change SID and service name for third-party applications	4	ALL	ALL	YES
2.6.1	Audit third party and home grown applications authentication systems	3	ALL	ALL	
3.	Oracle Access Controls				
3.1.1	Audit <i>utl_file_dir</i> parameter	3	ALL	ALL	YES
3.1.2	Audit <i>dbms_backup_restore</i> package permissions	3	ALL	ALL	YES
3.1.3	Audit Java access to the O/S	2	ALL	>= 8	YES
3.1.4	Be aware of how Java and Oracle interact	2	ALL	>= 8	YES
3.1.5	Secure Oracle Con Text	3	ALL	>= 8	YES
3.1.6	Remove oo4o if not needed	2	ALL	>= 7	YES
3.2.1	Secure ALL_USERS view	3	ALL	ALL	YES
3.2.2	Secure all ALL_% views	4	ALL	ALL	YES
3.3.1	Make <i>extproc</i> secure	2	ALL	>= 8	YES
3.4.1	Understand Data Access Descriptor administration	4	ALL	9i/AS	YES
3.5.1	Secure access to catalog roles	3	ALL	ALL	YES
3.5.2	Secure access to dba role views	3	ALL	ALL	YES
3.5.3	Password protect admin roles	4	ALL	ALL	YES
3.5.4	Check role hierarchy depth	4	ALL	ALL	
3.5.5	Adopt role naming conventions	5	ALL	ALL	
3.5.6	Create a role to manage users accounts	5	ALL	ALL	YES
3.6.1	Check database in archive log mode (if required)	3	ALL	ALL	
3.6.2	Check <i>user_dump_dest</i> is valid	4	ALL	ALL	YES
3.6.3	Check <i>background_dump_dest</i> is valid	4	ALL	ALL	YES

3.6.4	Check <i>core_dump_dest</i> is valid	4	ALL	ALL	YES
3.6.5	Check that <i>global_names</i> is true	3	ALL	ALL	YES
3.6.6	Check that <i>log_archive_start</i> is set to true	4	ALL	ALL	YES
3.6.7	Check that <i>max_enabled_roles</i> is set correctly	3	ALL	ALL	YES
3.6.8	Check that <i>os_authent_prefix</i> is set to "" (null string).	2	ALL	ALL	YES
3.6.9	Check that <i>os_roles</i> is set to false	4	ALL	ALL	YES
3.6.10	Check that <i>O7_dictionary_accessibility</i> is set to false	1	ALL	ALL	YES
3.6.11	Check that <i>remote_os_authent</i> is set to false	3	ALL	ALL	YES
3.6.12	Check that <i>remote_os_roles</i> is set to false	1	ALL	ALL	YES
3.6.13	Periodically confirm parameters in database are the same as the configuration file	3	ALL	ALL	
3.6.14	Audit use of IFILE and the contents of files pointed to by IFILE	3	ALL	>= 9i	
3.6.15	Check that <i>remote_listener</i> is null	3	ALL	>= 9i	YES
3.6.16	Check that <i>pfile</i> and <i>spfile</i> can only be written to and read by the software owner.	2	ALL	ALL	YES
3.6.17	Check that exempt access policy privilege is revoked	2	ALL	>= 9i	YES
3.6.18	Check record locking parameters	2	ALL	ALL	YES
3.6.19	Check for SQL92 security standards	2	ALL	ALL	YES
3.7.1	Check for non <i>sys</i> objects in system tablespace	1	ALL	ALL	YES
3.8.1	Check for users who have <i>dba</i> privilege	1	ALL	ALL	YES
3.8.2	Check for users or roles granted ALL PRIVILEGES	1	ALL	ALL	YES
3.8.3	Check for privileges with ANY keyword granted	1	ALL	ALL	YES
3.8.4	Check for privileges granted "WITH ADMIN"	2	ALL	ALL	YES
3.8.5	Check for privileges granted "WITH GRANT"	2	ALL	ALL	YES
3.8.6	Review system privileges granted	1	ALL	ALL	YES
3.8.7	Check for application objects owned by privileged users	2	ALL	ALL	YES
3.8.8	Check for direct access granted to tables and objects	2	ALL	ALL	YES
3.8.9	Check for "CREATE LIBRARY" privilege	1	ALL	ALL	YES
3.8.10	Use roles to access underlying database objects	3	ALL	ALL	YES
3.8.11	Audit access privileges on objects	2	ALL	ALL	YES
3.8.12	Use Integrity constraints	3	ALL	ALL	
3.8.13	Use triggers to insert critical data	3	ALL	ALL	
3.8.14	Restrict users to one role at once	2	ALL	ALL	
3.8.15	Check for users with "BECOME USER" privilege	2	ALL	ALL	YES
3.8.16	Check for CREATE ANY DIRECTORY privilege	2	ALL	>=9i	YES
3.8.17	Check for CREATE JOB privilege	2	ALL	>=10g	YES
3.9.1	Audit EXTERNAL users	2	ALL	ALL	YES
3.9.2	Check for external users who are <i>dba</i>	1	ALL	ALL	YES
3.9.3	Check for external users who have "ALL PRIVILEGES"	1	ALL	ALL	YES
3.9.4	Ensure external users have the least privileges possible	2	ALL	ALL	
3.9.5	Do not use remote host based authentication	2	ALL	ALL	YES
3.9.6	Check that no external users have SYSDBA or SYSOPER	1	ALL	ALL	YES
3.10.1	Revoke public execute privilege on <i>utl_file</i>	1	ALL	>= 8	YES
3.10.2	Revoke public execute privilege on <i>utl_tcp</i>	1	ALL	>=8.1.7	YES
3.10.3	Revoke public execute privilege on <i>utl_http</i>	1	ALL	>=8.1.7	YES
3.10.4	Revoke public privilege on <i>utl_sntp</i>	1	ALL	>=8.1.7	YES
3.10.5	Audit public execute privileges on <i>sys</i> owned packages.	1	ALL	ALL	YES
3.10.6	Revoke the public execute privilege on <i>dbms_random</i> .	2	ALL	ALL	YES
3.10.7	Revoke the public execute privilege on <i>dbms_lob</i>	1	ALL	>= 8i	YES
3.10.8	Revoke any privileges on <i>dbms_sql</i> and <i>dbms_sys_sql</i> granted	1	ALL	ALL	YES

3.10.9	Audit packages available via a database link	1	ALL	ALL	
3.10.10	Use invokers rights PL/SQL procedures	2	ALL	ALL	
3.10.11	Audit DIRECTORY objects	2	ALL	>= 8	YES
3.10.12	Revoke execute privileges on <i>sys.initjvmaux</i>	2	ALL	ALL	YES
3.10.13	Revoke public execute privilege on <i>dbms_job</i>	2	ALL	ALL	YES
3.10.14	Revoke public execute privilege on <i>dbms_scheduler</i>	1	ALL	>=10g	YES
3.10.15	Revoke public execute privilege on <i>owa_util</i>	2	ALL	ALL	YES
3.11.1	Audit directly granted privileges	2	ALL	ALL	
3.11.2	Access tables through packages or roles.	4	ALL	ALL	
3.12.1	Change <i>system</i> users default tablespace.	1	ALL	ALL	YES
3.12.2	Change users default and temporary tablespaces	2	ALL	ALL	YES
3.13.1	Revoke the RESOURCE role from users	1	ALL	ALL	YES
3.13.2	Revoke the CONNECT role from all users	2	ALL	ALL	YES
3.13.3	Add passwords to critical and administrative roles	3	ALL	ALL	
3.13.4	Revoke all non-essential rights from PUBLIC	3	ALL	ALL	
3.14.1	Set password lifetime in profile to 60	3	ALL	>= 8	
3.14.2	Set password grace time to 3	3	ALL	>= 8	
3.14.3	Set password reuse max to 20	2	ALL	>= 8	
3.14.4	Set failed login attempts to 5	3	ALL	>= 8	
3.14.5	Set up profiles for each class of database user	3	ALL	ALL	
3.14.6	Set up general profile parameters	2	ALL	ALL	
3.15.1	Set <i>_trace_files_public</i> to false	3	ALL	ALL	
3.15.2	Review hidden initialisation parameters	3	ALL	ALL	
3.15.3	Ensure system triggers fire	1	ALL	>=8i	YES
3.16.1	Objects in application tablespaces not owned by schema owner should be dropped	3	ALL	ALL	
3.17.1	Audit quota use per user	3	ALL	ALL	YES
3.17.2	Establish different users for schema management and data management	3	ALL	ALL	YES
3.18.1	Set up naming conventions for schema owners and administrators and users	5	ALL	ALL	
3.19.1	Audit users database triggers	2	ALL	ALL	YES
3.20.1	Audit access to critical sys owned views like user\$, link\$ etc	1	ALL	ALL	YES
3.20.2	Audit access to all dba and sys owned views	1	ALL	ALL	YES
3.20.3	Revoke SELECT ANY TABLE	1	ALL	ALL	
3.21.1	Revoke object creation privileges from all but schema owners and DBA's	2	ALL	ALL	YES
3.21.2	Ensure users can only see the objects they need	2	ALL	ALL	YES
3.22.1	Audit views to ensure only select access is allowed	2	ALL	ALL	YES
3.23.1	Reduce the chance of brute force attacks	2	ALL	ALL	
3.24.1	Prevent the dba reading system tables	2	ALL	ALL	YES
3.25.1	Prevent the dba from reading application data	4	ALL	ALL	
3.26.1	Audit integration and server to sever communications	2	ALL	ALL	
3.27.1	Audit internet access to the Oracle database	2	ALL	>=9iR2	YES
3.28.1	Audit and secure <i>statspack</i>	2	ALL	>= 8i	YES
4.	Auditing				
4.1.1	Configure audit and storage.	2	ALL	ALL	
4.2.1	Audit insert failures on critical objects	2	ALL	ALL	
4.2.2	Use triggers to capture login events	2	ALL	ALL	YES
4.3.1	Audit create session	2	ALL	ALL	YES
4.3.2	Audit use of all grant privileges.	2	ALL	ALL	YES
4.3.3	Audit the use of all drop statements	3	ALL	ALL	

4.3.4	Audit the use of all alter statements	2	ALL	ALL	
4.3.5	Audit the use of create user	3	ALL	ALL	YES
4.3.6	Audit use of create role	3	ALL	ALL	
4.3.7	Audit all create statements	3	ALL	ALL	
4.3.8	Establish procedures to review audit logs	3	ALL	ALL	YES
4.3.9	Use Log Miner to audit in the case of forensics	4	ALL	ALL	
4.4.1	Configure basic audit	2	ALL	ALL	
4.4.2	Limit users who can change the audit trail	2	ALL	ALL	YES
4.4.3	Protect the audit trail	2	ALL	ALL	YES
4.4.4	Backup the audit trail	3	ALL	ALL	YES
4.4.5	Purge the audit trail	4	ALL	ALL	YES
4.4.6	Audit all SYS operations	1	ALL	>=9iR2	YES
4.5.1	Check date / time stamps on database objects	3	ALL	ALL	
4.6.1	Ensure reports and alerts are in place to deal with irregularities found through audit	3	ALL	ALL	YES
4.7.1	Use triggers for row level auditing	3	ALL	ALL	
4.7.2	Use VPD, RLS and label security for full data protection	3	ALL	>= 8	
4.8.1	Be aware of possible failure to be alerted of suspicious activities	2	ALL	ALL	YES
4.9.1	Be aware of possible failure to audit the security profile.	2	ALL	ALL	
4.10.1	Audit and review the Oracle generated log files	2	ALL	ALL	
5.	Networking				
5.1.1	Prevent set commands on the listener	1	ALL	ALL	YES
5.1.2	Prevent remote dba access on sql*net v1	4	ALL	ALL	
5.1.3	Audit the <i>listener.ora</i> file	5	ALL	ALL	
5.1.4	Enable shared sockets	3	win	ALL	
5.1.5	Force the MTS dispatcher to use specific ports	4	ALL	ALL	
5.1.6	Do not use the standard listener ports 1521, 1526	2	ALL	ALL	YES
5.1.7	Do not use known SID or service names such as ORCL	2	ALL	ALL	YES
5.1.8	In small environments do not use hostnames in <i>listener.ora</i> .	2	ALL	ALL	
5.1.9	Use a personal firewall on database administrator computers	2	ALL	ALL	YES
5.1.10	Secure <i>listener.ora</i> at the O/S level	2	ALL	ALL	YES
5.1.11	Ensure that listener logging is enabled	2	ALL	ALL	YES
5.2.1	Restrict sources of database connections	3	ALL	ALL	
5.2.2	Use connection manager and Oracle names to restrict connections by source	2	ALL	ALL	
5.3.1	Set the listener password	1	ALL	ALL	YES
5.4.1	Restrict listener banner information	3	ALL	ALL	
5.5.1	Use a firewall to protect the Oracle server.	2	ALL	ALL	
5.6.1	Audit Oracle client file permissions	4	ALL	ALL	
5.6.2	Audit client configuration file contents	5	ALL	ALL	
5.6.3	Audit the listener	2	ALL	ALL	YES
5.7.1	Audit database links for hard clear text passwords	1	ALL	ALL	YES
5.7.2	Discover what objects can be seen in the linked database	2	ALL	ALL	YES
5.7.3	Create a policy to manage database links	1	ALL	ALL	YES
5.7.4	Database link user should not be a dba	1	ALL	ALL	YES
5.7.5	Audit what links exist into and from the database	1	ALL	ALL	YES
5.8.1	Confirm the file permissions in the network admin directory	2	ALL	ALL	YES
5.8.2	Add only minimum configuration files to all clients	2	ALL	ALL	
5.9.1	Keep up to date with Oracle listener vulnerabilities and patch	2	ALL	ALL	
5.10.1	Secure remote dba access to the server	1	ALL	ALL	

5.10.2	Use an application gateway firewall	2	ALL	ALL	
5.11.1	Set server to dedicated in the tnsnames.ora file	1	ALL	ALL	YES
5.11.2	Disable Oracle ports that are not needed.	3	ALL	ALL	YES
5.12.1	Audit the intelligent agent	2	ALL	ALL	YES
5.12.2	Protect clear text passwords for SNMP	2	ALL	ALL	YES
5.13.1	Use Oracle advance security to encrypt data transfer	3	ALL	ALL	
5.13.2	Enable SSL to protect client transmissions	3	ALL	ALL	
6.	Availability / backup / Recovery				
6.1.1	Review and document backup and restore procedures	3	ALL	ALL	YES
6.1.2	Review and document recovery procedures	3	ALL	ALL	YES
6.1.3	Store backup media off site	3	ALL	ALL	YES
6.1.4	Schedule cold backups	3	ALL	ALL	YES
6.1.5	Validate the backup media regularly	3	ALL	ALL	YES
6.1.6	Do not allow backups to be available on-line	2	ALL	ALL	
6.1.7	Create and use media retrieval procedures	2	ALL	ALL	
6.2.1	Mirror the on line redo logs	2	ALL	ALL	YES
6.3.1	Ensure the database is in archive log mode	2	ALL	ALL	YES
6.3.2	Ensure archive log directories exist and are protected	2	ALL	ALL	YES
6.3.3	Ensure archive logs are written to backup and are purged	3	ALL	ALL	YES
6.4.1	Separate the Oracle software from data and from on-line redo and archive	3	ALL	ALL	YES
6.4.2	Keep Oracle data files on separate disks	3	ALL	ALL	YES
6.4.3	Use OFA	5	ALL	ALL	
6.4.4	Use striping and mirroring or RAID for Oracle data	4	ALL	ALL	
6.5.1	Magnetically wipe old disks that have contained database data.	2	ALL	ALL	
6.6.1	Document and review disaster recovery procedures	4	ALL	ALL	YES
6.6.2	Include business users in disaster recovery planning	4	ALL	ALL	YES
7.	Application Development				
7.1.1	Identify and <i>wrap</i> all PL/SQL code in the database	2	ALL	ALL	YES
7.1.2	Checksum all PL/SQL objects in the database	3	ALL	ALL	
7.1.3	Audit PL/SQL code for hard coded usernames and passwords	3	ALL	ALL	
7.1.4	Audit PL/SQL code for possible SQL injection attacks	2	ALL	ALL	
7.1.5	Ensure as little information as possible about schema structure is available from the code in Oracle	3	ALL	ALL	
7.1.6	Pre-compile Java code before loading into the database	3	ALL	ALL	YES
7.2.1	Review which applications access the database and how and from where	2	ALL	ALL	
7.2.2	Implement procedures to limit which applications can access the database and from where	2	ALL	ALL	
7.2.3	Limit administration tools from accessing the database	3	ALL	ALL	
7.3.1	When decommissioning old applications remove all binaries and files	4	ALL	ALL	
7.4.1	Review procedures for adding new applications	4	ALL	ALL	
7.5.1	Establish procedures for movers, leavers and joiners	2	ALL	ALL	
7.6.1	Audit application file permissions	3	ALL	ALL	
7.7.1	Check for evidence of development on production databases	3	ALL	ALL	
7.8.1	Restrict ad-hoc queries against production database	3	ALL	ALL	
7.9.1	Review users permissions in test and development databases	2	ALL	ALL	
7.9.2	Check for database links with access to production databases from development or test systems	2	ALL	ALL	
7.9.3	Ensure "live" data held in test or development is mangled or obfuscated.	2	ALL	ALL	
7.9.4	Do not locate test and development databases on the same server as production	2	ALL	ALL	
7.9.5	Ensure there is no access from test and development to production	2	ALL	ALL	
7.9.6	No developer access to production	1	ALL	ALL	YES

7.9.7	No developer database accounts should exist on production database	2	ALL	ALL	
7.9.8	Backups and exports copy passwords to test and development – ensure they are not the same	2	ALL	ALL	
7.9.9	Place development and test on different network segment to production	2	ALL	ALL	
7.10.1	Move all non application objects from application tablespaces	2	ALL	ALL	
7.10.2	Ensure no privileged user owns application objects	2	ALL	ALL	
7.11.1	Audit resources used by the database	2	ALL	ALL	
7.12.1	Do not duplicate Oracle authentication	1	ALL	ALL	
7.12.2	Do not use one database login to authenticate all other users	2	ALL	ALL	
7.13.1	Do not use schema owners for administration tasks	2	ALL	ALL	
7.13.2	Ensure the schema owner is not a dba	2	ALL	ALL	
7.13.3	Lock schema owner accounts	2	ALL	ALL	
7.14.1	Audit public synonyms	5	ALL	ALL	
7.15.1	Do not hard code usernames and passwords in application source code	2	ALL	ALL	
7.15.2	Consider not using Java	2	ALL	>= 8	
7.15.3	Do not allow applications to change the schema	2	ALL	ALL	
7.16.1	Batch processes should access the database through one designed account	1	ALL	ALL	
7.16.2	Do not use external accounts for batch processes	1	ALL	ALL	
7.16.3	Consider password retrieval and use in schedulers	1	ALL	ALL	
7.16.4	Enable batch database accounts only when needed	1	ALL	ALL	
7.17.1	Use product user profile to secure SQL*Plus	4	ALL	ALL	
7.17.2	Audit query tool privileges	3	ALL	ALL	
7.18.1	Encrypt critical data	2	ALL	ALL	
7.19.1	Audit generated applications for known weaknesses	2	ALL	ALL	
7.19.2	Audit public libraries used for know vulnerabilities	2	ALL	ALL	
7.20.1	Use change control	2	ALL	ALL	
7.21.1	Audit use of advance queues	2	ALL	ALL	
7.22.1	Audit tools used for password leakage	2	ALL	ALL	
7.23.1	Ensure no tool offers better access to the database than the application	2	ALL	ALL	
7.24.1	Checksum application files for Trojans	2	ALL	ALL	
7.25.1	Start the Oracle HTTP Server as a non privileged user	1	ALL	>= 9i	YES
7.25.2	Configure HTTPS and secure the listener	3	ALL	>= 9i	YES
7.25.3	Add authentication for users	2	ALL	>= 9i	YES
7.25.4	Set HTTP passwords	2	ALL	>= 9i	YES
7.25.5	Configure product user profile for iSQL*Plus	3	ALL	>= 9i	YES
7.25.6	Restrict databases that can be accessed	2	ALL	>= 9i	YES
7.25.7	Disable iSQL*Plus on production servers	1	ALL	>= 9i	YES
7.26.1	Review how to enable and disable various database access features e.g.: IFS	2	ALL	ALL	
7.27.1	Protect debugger interfaces	2	ALL	ALL	
7.28.1	Do not divulge system information to the public	2	ALL	ALL	YES
8.	Application Servers and the Middle Tier				
	<i>Oracle Portal</i>				
8.1.1	Secure the portal DAD admin page	2	ALL	9iAS	YES
8.1.2	Encryption of the DAD password	1	ALL	9iAS	YES
8.1.3	Secure the portal users passwords in the database	1	ALL	9iAS	YES
8.1.4	Restrict the portal gateway URL	2	ALL	9iAS	YES
8.1.5	Remove the portal example programs	1	ALL	9iAS	YES
8.1.6	Revoke DBA from portal admin database users	1	ALL	9iAS	YES
8.1.7	Restrict access to OWA_UTL and other PL/SQL packages	1	ALL	9iAS	YES

8.2.1	Oracle Wireless Portal Create secure wireless user and password	3	ALL	9iAS	YES
	Oracle Web Cache				
8.3.1	Check permissions on file containing Webcache admin password	1	ALL	9iAS	YES
8.3.2	Check permissions on Webcache.xml	1	ALL	9iAS	YES
	Oracle iCache				
8.4.1	Reset default account passwords in database cache database	1	ALL	9iAS	YES
8.4.2	Check permissions for export files used to create database cache	2	ALL	9iAS	YES
	Apache				
8.5.1	Protect Apache	2	ALL	9iAS	YES
8.5.2	SYSTEM password appears in Apache install window title	3	ALL	9iAS	YES
8.5.3	Change default port numbers	3	ALL	9iAS	YES
8.5.4	Apply security patches to web server	1	ALL	9iAS	YES
8.5.5	Run <i>nessus</i> against 9iAS	4	ALL	9iAS	YES
8.5.6	Protect <i>httpd.conf</i> file	1	ALL	9iAS	YES
8.5.7	Remove OJSP example programs	1	ALL	9iAS	YES
8.5.8	Protect against an attacker reading JSP class files	1	ALL	9iAS	YES
8.5.9	Restrict dynamic monitoring services	1	ALL	9iAS	YES
	Oracle Internet File Server				
8.6.1	Change IFS password	1	ALL	9iAS	YES
	Oracle Reports Server				
8.7.1	Secure the reports sever	1	ALL	9iAS	YES
8.7.2	Use only compiled reports	2	ALL	9iAS	YES
8.7.3	Rename <i>rwcgi60</i> executable	3	ALL	9iAS	YES
	XML/XSL and the XSQL Servlet				
8.8.1	Protect XMLConfig.xml	3	ALL	9iAS	YES
8.8.2	Delete servlet class files	2	ALL	9iAS	YES
8.8.3	Disable servlet URL	3	ALL	9iAS	YES
8.8.4	Delete XSQL examples	3	ALL	9iAS	YES
8.8.5	In XSQL use bind variables	3	ALL	9iAS	YES
8.8.6	Set allow-client-style=no in XMLConfig.xml	3	ALL	9iAS	YES
8.8.7	Delete the XSQL XDK from production databases	2	ALL	9iAS	YES
8.8.8	Restrict the XSQL status URL	3	ALL	9iAS	YES
8.8.9	Change the mapping for the servlet URL	3	ALL	9iAS	YES



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

Hong Kong Advanced Forensics Seminar	Hong Kong, Hong Kong	Nov 09, 2009 - Nov 14, 2009	Live Event
SANS Sydney 2009	Sydney, Australia	Nov 09, 2009 - Nov 14, 2009	Live Event
SANS Vancouver 2009	Vancouver,	Nov 14, 2009 - Nov 19, 2009	Live Event
SecurityByte 2009	New Delhi, India	Nov 17, 2009 - Nov 20, 2009	Live Event
SANS Geneva CISSP at HEG 2009 Autumn	Geneva, Switzerland	Nov 23, 2009 - Nov 28, 2009	Live Event
SANS London 2009	London, United Kingdom	Nov 28, 2009 - Dec 06, 2009	Live Event
SANS WhatWorks in Incident Detection Summit 2009	Washington, DC	Dec 09, 2009 - Dec 10, 2009	Live Event
SANS CDI East 2009	Washington, DC	Dec 11, 2009 - Dec 18, 2009	Live Event
SANS WhatWorks in Data Leakage Prevention and Encryption Summit 2010	New Orleans, LA	Jan 07, 2010 - Jan 12, 2010	Live Event
SANS Security East 2010	New Orleans, LA	Jan 10, 2010 - Jan 18, 2010	Live Event
SANS AppSec 2010 and WhatWorks in AppSec Summit	San Francisco, CA	Jan 29, 2010 - Feb 05, 2010	Live Event
SANS San Francisco 2009	OnlineCA	Nov 09, 2009 - Nov 14, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced