Global Information Assurance Certification Paper

ORACLE DATABASE AUDITING
Oracle 8.x

SANS GSNA PRACTICAL ASSIGNMENT
Version 1.1 (amended AUG 21 3001)

GARETH PRICE

Introduction

The Oracle product portfolio has at its core a relational database engine, the data in this database is made available via a number of ancillary products. The SQL language provides the interface to the structure of the database and the data stored in it. SQL*Net makes the database available over the network using a variety of network transport protocols including TCP/IP. Oracle Application Server makes the database available over the World Wide Web.

Access to the Oracle database is controlled in a number of ways. The underlying operating system protects the core application and data files; it can also help protect the network connectivity to the computer running Oracle. The Oracle database contains control mechanisms to protect the data within it. Key components are Users, Schemas, Roles, Privileges and Profiles.

Oracle has built-in audit facilities and has a lot of functionality that can be used to produce customized auditing of your database. Despite the widespread use of this product there isn't much material available relating to auditing.

Research in Audit, Measurement Practice and Control

Current State of Practice in Oracle Auditing

There is a lot of documentation on auditing in general and auditing operating systems. There is very little material on auditing Oracle databases.

Descriptions of Facilities Available

I found several sources describing what is available in an Oracle database to make it secure including the documentation produced by Oracle. The main Oracle references to security and auditing are in:

Oracle8 Concepts [7]
- Chapter 26 Privileges and Roles
- Chapter 27 Auditing
- Chapter 28 Database Recovery
- Chapter 30 Distributed Databases

Oracle8 Admin Guide [8]
- Chapter 18 Managing Rollback Segments
- Chapter 19 Establishing Security Policies
- Chapter 20 Managing Users and Resources
- Chapter 22 Auditing Database Use

The book "Oracle Security" [1] contains a shorter and more accessible introduction to the parts of Oracle relevant to security and auditing.

Free Manual Methodologies

"Hack Proofing Oracle" [4] starts out as an audit methodology and ends as a set of features to use. There were only 10 audit steps listed and of these five could be objectively measured.

"Oracle Security" [1] does not contain an explicit audit methodology but one can be extracted from the hints and tips contained in the text. The material in this book will be used to suggest improvements to the ISS audit methodology.

The current Oracle 7 HOWTO [3] and Oracle 8 HOWTO [4] from the Linux Documentation Project focus on getting an installation running rather than securing it. They refer to changing the default passwords for SYS and SYSTEM, creating a directory for auditing data and the Oracle 8 one refers to SQL*Net allowing unauthenticated logons.

Free Automatic Tools

Nessus [5] & [6] contains six tests to run against an Oracle database, they are all aimed at unauthenticated network accessible services. They test the version of the Listener, whether the Listener has a password set, whether the Web Server can be crashed, whether the Application Server can be overflowed, whether XSQL executes arbitrary Java and whether XSQL executes arbitrary SQL.

Commercial Manual Methodologies

I could not find a commercial manual methodology to audit an Oracle database.

Commercial Automatic Tools

The only automatic audit method I found is the Internet Security Systems Database Scanner [9] &[10]. This is an expensive product and I only have access to the evaluation version that allows configuration but not scanning. I will create a configuration but perform my own interpretation of each test as part of a manual audit.

Why Current Methods and Techniques Need Improvement

Objective Test Improvements

The ISS Database Scanner tool has not been updated nearly as much as the more popular Security Scanner [12]. I could only find one update file on the ISS web site, that is in stark contrast to the 23 updates and 5 other checks for the current version of Internet Scanner and 16 updates for Security Scanner. This is possibly because the tests performed by the tool do not go out of date.

It makes one reference to Oracle software patches and does not include security vulnerabilities tested for by Nessus. Software patches are an important, if unglamorous, part of maintaining a secure system. Also if the database crashes because of a known fixed bug that has not been patched it is as devastating as if a malicious person damaged the database.

There is no reference to the physical disk locations of the control, data and log files that make up the database. It is important for system integrity and performance that these files are spread across available system disks. This is most important for the control files where at least one must survive disk problems to allow the database to be accessible.

Database backups are checked on MS SQL Server but not on Oracle, despite information being available in the SYS.INCEXP tables SYS.INCFIL tables.

Suggested extra objective tests taken from "Oracle Security"[1]:

Test	Detailed Description	Non-Compliant if …
Scott Account	Does the default Scott account exist	Scott account exists
Objects in user schemas	Are there any Objects in application user schemas	Tables, views, packages, procedures, functions or triggers exist in application user schemas

Failed NT logons	NT Event logs relating to failed logons for accounts using NT OS Authentication	More than number allowed in security policy.

Suggested extra objective tests taken from "Hack Proofing Oracle"[2]:

Test	Detailed Description	Non-Compliant if …
Default accounts locked	Check that default accounts locked	Any default accounts not locked
Listener ports visible	Are listener ports filtered at firewall according to security policy	Listener ports not filtered at firewall as defined in security policy
Net8 IP address filtering	Is Net8 configured to only respond to IP Addresses defined in security policy	Net8 not configured to filter incoming IP connections as defined in security policy
Unused software	Are unused software options removed from the system	Unused software options installed on system
Roles granted to PUBLIC	Are there any Roles granted to PUBLIC	Any roles exist granted to PUBLIC
Package contents hidden using PLSQL WRAP	Is PLSQL WRAP used to hide contents of packages	Package code in plain text
UTL_SMTP availability	Is UTL_SMTP available to unsuitable accounts	UTL_SMTP available to accounts not defined in security policy
UTL_TCP availability	Is UTL_TCP available to unsuitable accounts	UTL_TCP available to accounts not defined in security policy
UTL_HTTP availability	Is UTL_HTTP available to unsuitable accounts	UTL_HTTP available to accounts not defined in security policy
Use of Oracle Advanced Security	Is Oracle Advanced Security used for network encryption	Oracle Advanced Security not used for network encryption when this is required by security policy

Suggested extra objective tests performed by "Nessus Plug-In" [5] & [6]:

Test	Detailed Description	Non-Compliant if …
TNS listener version	What version of Oracle TNS listener is running	TNS Listener reports version 7.3.4, 8.0.6, or 8.1.6
Oracle XSQL Sample Application	See if the Sample Oracle XSQL Application allows execution of arbitrary SQL query	Sample Oracle XSQL Application allows execution of arbitrary SQL query
TNS Listener password protected	Is the Oracle TNS listener password protected	TNS Listener reports SECURITY=OFF meaning no password protection
Oracle XSQL Stylesheet Vulnerability	See if a test Oracle XSQL page allows inclusion of user defined stylesheet	Test Oracle XSQL page airport.xsql allows inclusion of user defined stylesheet

Oracle Web Server denial of Service	See if the Oracle Web Server can be crashed by sending a large request string	Oracle Web Server crashes when sent a large request string
Oracle Application Server Overflow	See if the Oracle Application Server can be attacked with an overflow	Oracle Application Server can be attacked with an overflow

Subjective Test Improvements

Suggested extra subjective tests taken from "Hack Proofing Oracle" [2]:

Test	Detailed Description	Non-Compliant if …
DBMS_RANDOM	Is DBMS_RANDOM used for cryptography applications	Random number generator code found in application where DBMS_RANDOM could be used.
UTL_FILE lacks application segregation	UTL_FILE no distinguishing between callers so appa can write over appb data	Application with a need for mandatory file segregation using UTL_FILE

What Can be Measured Objectively

The following are extracted from the ISS Database Scanner software [12] and edited for brevity.

Test	Detailed Description	Platform
Account Permissions	Check for privileges granted to accounts – violations for those not in your specified list	All
Audit Table Permissions	Check that only the appropriate accounts have permissions on the table where the audit data is stored (SYS.AUD$).	All
Audit Table Tablespace	Check that the audit trail table (SYS.AUD$) has not been installed in the system tablespace.	All
Audit Trail Location	Check the audit trail destination against policy of OS or DB	All
Auditing of Commands	Check that system-wide auditing of statements and privileges is configured in accordance with specified policy.	All
Auditing of Schema Objects	Collect object auditing configuration.	All
Composite Resource Usage Limit	Check that profiles do not exceed the specified Composite Resource Usage parameter.	All

Concurrent Sessions Resource Usage Limit	Check that profiles do not exceed the specified Concurrent Sessions Resource Usage parameter.	All
Connect Time Resource Usage Limit	Check that any existing profiles have Connect Time Resource Usage limits within the range allowed by the policy.	All
CPU/Call Resource Usage Limit	Check that any existing profiles have CPU/Call Resource Usage limits within the range allowed by the policy.	All
CPU/Session Resource Usage Limit	Check that any existing profiles have CPU/Session Resource Usage limits within the range allowed by the policy.	All
Data Dictionary Accessibility	Check that the parameter O7_DICTIONARY_ACCESSIBILITY is set to false.	All
Database Link Password Encryption	Check that the database link password encryption is set to TRUE or FALSE according to policy	All
Database Link Password Unencrypted	Check that database link passwords are not stored in clear text.	All
Database Link Permissions	Check for accounts with permissions to view the table SYS.LINK$.	All
DBA Includes Non-default Account	Check for non-default members in the DBA role.	All
Default Accounts and Passwords	Check for default passwords that have not been changed.	All
Default Internal Password	Check that the internal password used to connect as internal has been changed from the default installation value ORACLE.	All
Default Listener Password	Check the listener.ora file to verify that the default listener password has been changed and is not blank.	All
Default Password Verify Function	Check that the default password verify function, VERIFY_FUNCTION, has not been modified.	Oracle 8.0 and above

Default SAP Account and Password	Check that the default SAP password has been changed.	All
Default SNMP Account	Check that the default SNMP password has been changed.	All
Default Tablespace	Check if accounts are using the SYS or SYSTEM tablespaces.	All
Excessive DBA Connections	Check that an excessive number of connections do not have the DBA role at the time the scan is executed.	All
Expired Passwords Found in Oracle 7	Check Oracle 7 servers for password expiration by looking for changes to password hash since last scan	Oracle 7
Expired Passwords Found in Oracle 8	Check that password ages do not exceed a reasonable password lifetime.	Oracle 8x
Failed Login Attempts	Check that any existing profiles have Failed Login Attempts limits within the allowed policy range.	All
File Checksums	Look for changes to the checksums for files in the $ORACLE_HOME\bin directory tree against the values recorded in the previous scan.	All
File Group	Check the $ORACLE_HOME directory and other Oracle common system files for group privileges other than dba.	All
File Modifications	Check for file size, date, file deletion and re-additions for all files in the $ORACLE_HOME directory to find file modifications.	All
File Owner	Check that all files in the $ORACLE_HOME directory and other Oracle common system files are owned by the Oracle software owner.	All
File Permissions	Check permissions on system files are Oracle software owner and group.	All
File Permissions listener.ora	Check the permissions of the operating system file listener.ora.	All
File Permissions snmp file	Check the snmp.ora or snmp_rw.ora files for weak permissions.	All
File Permissions strtSID.cmd	Check the permissions for the Oracle startup file. This file contains the internal password.	Oracle 8.0 and earlier on Windows NT

File Permissions SYSDBA password file	Check the permissions of the operating system file orapw<SID> (on Unix systems) or pwd<SID>.ora (on Windows NT systems).	All
Idle Time Resource Usage Limit	Check that any existing profiles have Idle Time Resource Usage limits within the range allowed by the policy.	All
Intelligent Agent Patch	Check that the Intelligent Agent patch is installed.	Oracle 8.x on Unix versions 8.0.3, 8.0.4, 8.0.5.0, 8.1.5
Internal Password in Spoolmain	Check to determine if the internal password has been logged in the spoolmain.log file during install.	Windows NT only
Listener Cleartext Password	Check for the listener password being stored in clear text.	All
Login Encryption Setting	Check that encryption of passwords is enabled when connecting to Oracle from a client.	All
Logon Hours Violations	Review audit logs for after hours connections.	All
Oracle Licensing Compliance	Check that licensing is enabled and the warning level has not been exceeded.	All
Oracle SQL92_SECURITY	Check that the SQL92_SECURITY parameter is enabled.	All
Oracle Wallet Permissions	Check the 'rwx' permissions on the Oracle sqlnet.ora file and the files in the Oracle Wallet directory.	Oracle 8.x
OS Authentication Prefix	Check that the OS_AUTHENT_PREFIX setting is in compliance with the policy.	All
Password Attacks	Check for evidence of password attacks by looking for failed logins in audit table.	All
Password Grace Time	Check that all profiles have a Password Grace Time within the limits of the policy.	All
Password Life Time	Check that Oracle 8 profiles have not exceeded the allowed limit for Password Life Time.	All
Password Lock Time	Check that Oracle 8 profiles have not exceeded the allowed limit for PASSWORD_LOCK_TIME.	All

Password Reuse Max	Check that Oracle 8 profiles have not exceeded the allowed limit for PASSWORD_REUSE_MAX.	All
Password Reuse Time	Check that Oracle 8 profiles are not within the allowed limit for PASSWORD_REUSE_TIME.	All
Password Verify Function	Check that the Password Verify Function is specified properly.	All
Password Verify Function Changes	Check for changes in the functions being used for password strength verification.	All
Private SGA Resource Usage Limit	Check that any existing profiles have Private SGA Resource Usage limits within the range allowed by the policy.	All
Privileged OS Users	Check for users that belong to operating system groups that give them access to the database with SYSDBA and/or SYSOPER privilege.	All
Privileges Granted With Admin	Check that privileges having the WITH ADMIN OPTION have not been granted.	All
PUBLIC Object Permissions	Check for object permissions granted to PUBLIC.	All
PUBLIC System Privileges	Check for system privileges granted to PUBLIC.	All
Reads/Call Resource Usage Limit	Check that any existing profiles have Reads/Call Resource Usage limits within the range allowed by the policy.	All
Reads/Session Resource Use Limit	Check that any existing profiles have Reads/Session Resource Usage limits within the policy allowed range.	All
Registry Permissions	Checks that the group 'Everyone' does not have permissions to any subkeys or values in the Oracle registry key.	Windows NT only
Remote Login Password File	Check that the Oracle parameter REMOTE_LOGIN_PASSWORDFILE is in compliance with the policy.	All
Resource Limits Not Enabled	Check that the configuration option RESOURCE_LIMIT is set to TRUE.	All
Role Passwords	Check for roles without passwords.	All
Role Permissions	Check that role permissions are in compliance with the policy. Aimed at detecting direct access to tables and sequences rather than through views and packages.	All

Roles Granted With Admin	Check for roles granted using the WITH ADMIN OPTION.	All
Setgid Bit	Check for Oracle files with the setgid bit enabled.	Unix only
Setuid Bit	Check if any Oracle files have the setuid bit enabled.	Unix only
Setuid Bit of File cmctl	Check if the file $ORACLE_HOME\bin\cmctl has the setuid bit on.	Unix only
Setuid Bit of File onrsd	Check if the file $ORACLE_HOME\bin\onrsd has the setuid bit enabled.	Unix only
Setuid Bit of File oracleO	Check if the file $ORACLE_HOME\bin\oracleO has the setuid bit enabled.	Unix only
Setuid Bit of File oratclsh	Check if the file $ORACLE_HOME\bin\oratclsh has the setuid bit enabled.	Unix only
Setuid Bit of File otrccref	Check if the file $ORACLE_HOME\bin\otrccref has the setuid bit on.	Unix only
Stale Accounts	Check for stale Oracle accounts by looking for logon records in audit table.	All
Trusting Remote OS Authentication Setting	Check that the REMOTE_OS_AUTHENT parameter is not set to TRUE.	All
Trusting Remote OS for Roles Setting	Check that the REMOTE_OS_ROLES parameter is not set to true	All
Unencrypted SNMP Password	Check to determine if the SNMP password is stored unencrypted in the snmp.ora or snmp_rw.ora file.	All
Use of CONNECT Default Role	Check that accounts have not been granted the CONNECT role.	All
Use of RESOURCE Default Role	Check that accounts have not been granted the RESOURCE role.	All
UTL_FILE Permissions	Check permissions on the UTL_FILE package.	All
UTL_FILE_DIR Setting	Check that the Oracle parameter UTL_FILE_DIR is not set to * to allow the UTL_FILE package permissions on all directories.	All
View Missing With Check Option	Check to see that any views which have been granted UPDATE or INSERT permissions contain the WITH CHECK option at the end of the WHERE clause.	All
Weak Account Passwords	Check that Oracle passwords are not easy to guess using dictionary and limited brute force guessing	All

Weak Internal Password	Check for a weak internal password using dictionary attack.	All
Weak Listener Passwords	Check for weak passwords in the listener.ora file using dictionary attack	All
Weak Passwords for SYSDBA/SYSOPER	Check that accounts with the SYSDBA or SYSOPER role do not have weak passwords using dictionary attack	All
Weak SNMP Password	Check for weak passwords in the SNMP file using dictionary attack	All
With Grant Option	Check for object privileges granted using the WITH GRANT OPTION.	All

What must be measured Subjectively

The following are extracted from the ISS Database Scanner software [12] and edited for brevity.

Test	Detailed Description	Platform
Audit Trail	Collect audit trail data for review using the audit trail report.	All

How do you know when your system is non-compliant

Objective Tests

The following are extracted from the ISS Database Scanner software [12] and edited for brevity.

Test	Non-Compliant if …	External Written Policy Required
Account Permissions	Privileges granted to accounts that aren't specified as allowed in policy.	
Audit Table Permissions	Accounts have permissions on the audit table (SYS.AUD$) which aren't specified in policy (apart from SYS and SYSTEM),	
Audit Table Tablespace	Audit trail table (SYS.AUD$) has been installed in the system tablespace.	
Audit Trail Location	Audit trail destination against policy of OS or DB	

Auditing of Commands	System-wide auditing of statements and privileges is not configured in accordance with specified policy of writing one record for each access or once per session for audit success and/or audit failure.	
Auditing of Schema Objects	Object auditing configuration is not in compliance with policy. This would usually be turned on for sensitive database objects or to investigate security problems.	
Composite Resource Usage Limit	A profile exceeds the Composite Resource Usage parameter specified in the policy.	
Concurrent Sessions Resource Usage Limit	A profile exceeds the specified Concurrent Sessions Resource Usage parameter specified in the policy.	
Connect Time Resource Usage Limit	A profile exceeds the Connect Time Resource Usage limits specified in the policy.	
CPU/Call Resource Usage Limit	A profile exceeds the CPU/Call Resource Usage limits specified in the policy.	
CPU/Session Resource Usage Limit	A profile exceeds the CPU/Session Resource Usage limits specified in the policy.	
Data Dictionary Accessibility	Parameter O7_DICTIONARY_ACCESSIBILITY is set to TRUE.	
Database Link Password Encryption	Database link password encryption is set to FALSE and database does NOT connect to any pre Oracle 7.2 databases	
Database Link Password Unencrypted	Database link passwords stored in SYS.LINK$ table.	
Database Link Permissions	Accounts have permissions to view the table SYS.LINK$ which aren't specified in policy (apart from SYS and SYSTEM),	
DBA Includes Non-default Account	Members in the DBA role which aren't specified in policy (apart from SYS and SYSTEM).	
Default Accounts and Passwords	Default passwords have not been changed on default accounts like SYS, SYSTEM, and SCOTT.	

Default Internal Password	Internal password has not been changed from the default installation value ORACLE.	
Default Listener Password	Default listener password in listener.ora has not been changed or it is blank.	
Default Password Verify Function	Default password verify function, VERIFY_FUNCTION, has been modified.	
Default SAP Account and Password	The default SAP password has not been changed.	
Default SNMP Account	The default SNMP password has not been changed.	
Default Tablespace	Accounts are using the SYS or SYSTEM tablespaces.	
Excessive DBA Connections	Users connected to the server at the time the scan is executed have the DBA role that are not specified in the policy.	
Expired Passwords Found in Oracle 7	Password hash values on Oracle 7 server have not been changed during maximum period defined in policy.	
Expired Passwords Found in Oracle 8	Password lifetime in a profile on Oracle 8 server exceeds lifetime defined in policy (including no lifetime set when limit specified in policy).	
Failed Login Attempts	Failed Login Attempts limit in a profile on Oracle 8 server exceeds limit defined in policy (including no limit set when limit specified in policy).	
File Checksums	Checksums for files in the $ORACLE_HOME\bin directory tree changed since previous scan.	
File Group	Files in $ORACLE_HOME directory and other Oracle common system files have group privileges different to Oracle software owner.	
File Modifications	File size or date changes, file deletion and file readditions for all files in the $ORACLE_HOME directory excluding database redo log files and data files.	
File Owner	Files in the $ORACLE_HOME directory and other Oracle common system files are not owned by the Oracle software owner.	
File Permissions	Permissions on system files are not just Oracle owner and extra permissions are not specified in policy. OR ‘Everyone’ has permissions on any of these files on NT.	
File Permissions listener.ora	Permissions on listener.ora are not just Oracle owner and extra permissions are not specified in policy. OR ‘Everyone’ has permissions on any of these files on NT.	

File Permissions snmp file	Permissions on snmp.ora or snmp_rw.ora are not just Oracle owner and extra permissions are not specified in policy. OR 'Everyone' has permissions on any of these files on NT.	
File Permissions strtSID.cmd	'Everyone' has permissions on Oracle startup file strSID.cmd on NT	
File Permissions SYSDBA password file	Permissions on orapw<SID> are not just Oracle owner and extra permissions are not specified in policy. OR 'Everyone' has permissions on pwd<SID>.ora on NT	
Idle Time Resource Usage Limit	Idle Time Resource Usage limit in a profile on Oracle 8 server exceeds limit defined in policy (including no limit set when limit specified in policy).	
Intelligent Agent Patch	Intelligent Agent patch not installed.	
Internal Password in Spoolmain	INTERNAL password has been logged in the spoolmain.log file during install on Windows NT.	
Listener Cleartext Password	Listener password being stored in clear text.	
Login Encryption Setting	Encryption of passwords is NOT enabled when connecting to Oracle from a client. ORA_ENCRYPT_LOGIN not set or set to FALSE.	
Logon Hours Violations	Connections in audit log at times that are not specified in policy.	
Oracle Licensing Compliance	Licensing is not enabled. LICENSE_MAX_USERS and LICENSE_MAX_SESSIONS are set to 0.	
Oracle SQL92_SECURITY	SQL92_SECURITY parameter is NOT enabled.	
Oracle Wallet Permissions	Permissions on sqlnet.ora file and the files in the Oracle Wallet directory are not just Oracle owner and group and extra permissions are not specified in policy. OR 'Everyone' has permissions on these files on NT	
OS Authentication Prefix	OS_AUTHENT_PREFIX setting is NOT in compliance with the policy.	
Password Attacks	Failed logins NOT being recorded in the audit table or more failed logins recorded in the audit table than allowed by policy.	
Password Grace Time	One or more profiles do NOT have a Password Grace Time within the limits of the policy (including no time set when time specified in policy).	
Password Life Time	One or more profiles do NOT have a Password Life Time within the limits of the policy (including no time set when time specified in policy).	

Password Lock Time	One or more profiles do NOT have a Password Lock Time within the limits of the policy (including no time set when time specified in policy).	
Password Reuse Max	Times password must change before old password can be reused. One or more profiles do NOT have a Password Reuse Max Limit within the limits of the policy (including no limit set when limit specified in policy).	
Password Reuse Time	Days that must elapse before an old password can be reused. One or more profiles do NOT have a Password Reuse Time Limit within the limits of the policy (including no time set when time specified in policy).	
Password Verify Function	Password Verify Function setting does not match policy. Setting is NULL when required. Setting is specified but not required. Setting is required and specified but PL/SQL function is not owned by SYS or PL/SQL function is not available on local database.	
Password Verify Function Changes	Function being used for password strength verification has changed since last scan.	
Private SGA Resource Usage Limit	One or more profiles do NOT have a Private SGA Resource Usage limit within the limits of the policy (including no time set when time specified in policy).	
Privileged OS Users	Unix or NT users in operating system groups that gives them access to the database with SYSDBA and/or SYSOPER privilege who are not listed in the policy. Unix group defined at database install and defaults to dba. For NT the groups are ORA_<sid>_DBA, ORA_<sid>_OPER, ORA_DBA, and ORA_OPER.	
Privileges Granted With Admin	Privileges have been granted with the WITH ADMIN OPTION.	
PUBLIC Object Permissions	Object permissions granted to PUBLIC.	Y
PUBLIC System Privileges	System privileges granted to PUBLIC.	Y
Reads/Call Resource Usage Limit	One or more profiles do NOT have a Reads/Call Resource Usage limit within the limits of the policy (including no limit set when limit specified in policy).	
Reads/Session Resource Use Limit	One or more profiles do NOT have a Reads/Session Resource Usage limit within the limits of the policy (including no limit set when limit specified in policy).	
Registry Permissions	NT group 'Everyone' has permissions to any subkeys or values in the Oracle registry key.	

Remote Login Password File	Oracle parameter REMOTE_LOGIN_PASSWORDFILE is NOT in compliance with the policy of NONE, EXCLUSIVE or SHARED.	
Resource Limits Not Enabled	Configuration option RESOURCE_LIMIT is set to FALSE.	
Role Passwords	One or more roles without passwords when roles specified as requiring passwords in policy.	
Role Permissions	Role permissions are NOT in compliance with the defined policy. Usually when there is direct access to tables and sequences rather than through views and packages.	
Roles Granted With Admin	One or more roles granted using the WITH ADMIN OPTION.	
Setgid Bit	Unix Oracle files with the setgid bit enabled.	
Setuid Bit	Unix Oracle files have the setuid bit enabled and they are not listed in the policy (usually not needed).	
Setuid Bit of File cmctl	Unix file $ORACLE_HOME\bin\cmctl has the setuid bit on and not listed in the policy.	
Setuid Bit of File onrsd	Unix file $ORACLE_HOME\bin\onrsd has the setuid bit enabled and not listed in the policy.	
Setuid Bit of File oracleO	Unix file $ORACLE_HOME\bin\oracleO has the setuid bit enabled and not listed in the policy.	
Setuid Bit of File oratclsh	Unix file $ORACLE_HOME\bin\oratclsh has the setuid bit enabled and not listed in the policy.	
Setuid Bit of File otrccref	Unix file $ORACLE_HOME\bin\otrccref has the setuid bit on.	
Stale Accounts	Stale Oracle accounts found by looking for logon records in audit table.	
Trusting Remote OS Authentication Setting	REMOTE_OS_AUTHENT parameter is set to TRUE.	
Trusting Remote OS for Roles Setting	REMOTE_OS_ROLES parameter is set to TRUE	
Unencrypted SNMP Password	SNMP password is stored unencrypted in the snmp.ora or snmp_rw.ora file.	
Use of CONNECT Default Role	Accounts have been granted the CONNECT role.	Y
Use of RESOURCE Default Role	Accounts have been granted the RESOURCE role.	Y

UTL_FILE Permissions	Users or Roles have permissions on the UTL_FILE package.	Y
UTL_FILE_DIR Setting	Oracle parameter UTL_FILE_DIR is set to *.	Y
View Missing With Check Option	One or more views have been granted UPDATE or INSERT permissions without the WITH CHECK option at the end of the WHERE clause.	
Weak Account Passwords	One or more Oracle passwords found using limited guessing based on account name and dictionary attack.	
Weak Internal Password	Weak internal password found using limited guessing based on account name and dictionary attack.	
Weak Listener Passwords	One or more weak passwords found in the listener.ora file using limited guessing based on account name and dictionary attack.	
Weak Passwords for SYSDBA/SYSOPER	Weak passwords found for accounts with the SYSDBA or SYSOPER role using limited guessing based on account name and dictionary attack	
Weak SNMP Password	Weak passwords found in the SNMP file using limited guessing based on account name and dictionary attack.	
With Grant Option	Object privileges granted using the WITH GRANT OPTION.	

Subjective Tests

The following are extracted from the ISS Database Scanner software [12] and edited for brevity.

Test	Non-Compliant if …	External Written Policy Required
Audit Trail	Items found in audit trail that are against policy. Examples would be unauthorised: Database changes creation of users or roles changes to auditing settings	Y

Application of Audit Techniques in the Real World

Conducting the Audit

A 'Custom' install of Oracle8i Enterprise Edition 8.1.6.0.0 Release 2 on Windows 2000 was used to see what problems the audit methodology found. Ideally this should have been a full install of release 8.1.7 but I did not have the software and disk space available. The install was performed while logged on as Administrator. In Oracle Installer all Oracle 8i Server, Oracle Net8, Oracle Utilities, Oracle Installation components were installed including options. The default Oracle JDBC components for JDK 1.1.8.1.6.0.0 were installed as well as Oracle Java tools.

I used the default database SID of ORCL, no options were configured for this database and it was set as 8.0.5 compatible. Archive log mode was enabled.

I created a default Net8 Listener configuration with a net service for my test ORCL database.

The tool allows different levels of testing from 2 to 7 as well as custom levels you can define yourself. Level 2 just checks passwords, registry permissions on NT and the setgid bit on Unix Oracle files. Level 7 enables most of the tests.

Tests enabled by default for Level 7 that I did not perform are:

Test
Expired passwords Found in Oracle 7
File permissions – strtSID.cmd
SetUID bit
SetGID bit
SetUID bit of File cmctl
SetUID bit of File onrsd
SetUID bit of File oracle0
SetUID bit of File oratclsh
SetUID bit of File otrccref
Weak Account Passwords
Weak Internal Passwords
Weak Listener Password
Weak SYSDBA/SYSOPER Passwords
Weak SNMP Password

Tests enabled by default for Level 7 that require parameters are:

Test	Default Parameter	New Parameter
Expired passwords Found in Oracle 8	30	101
Failed Login Attempts	5	4

Password Attacks	25	10
Remote Login Password File	NONE	NONE
Stale Accounts	30	30
Account Permissions	Select from Tables Select/ Insert/ Update/ Delete from Views and Synonyms Execute Packages and Functions	None allowed
Privileges granted with ADMIN	Exclude DBA, SYS and SYSTEM	Exclude DBA, SYS and SYSTEM
Role Permissions	Select/ Insert/ Update/ Delete from Views and Synonyms Execute Packages and Functions	Select/ Insert/ Update/ Delete from Views and Synonyms Execute Packages and Functions
Roles granted with ADMIN	Exclude DBA, SYS and SYSTEM	Exclude DBA, SYS and SYSTEM
Audit Trail Location	DB	DB
File Checksums	<ORACLE_HOME>/	<ORACLE_HOME>/
File group	<ORACLE_HOME>/	<ORACLE_HOME>/
File modifications	<ORACLE_HOME>/	<ORACLE_HOME>/
File Owner	<ORACLE_HOME>/	<ORACLE_HOME>/
File Permissions	755	Win NT N/A
File Permissions – listener.ora	755	Win NT N/A
File Permissions – snmp.ora snmp_rw.ora	755	Win NT N/A
File Permissions – pwdSID.ora	755	Win NT N/A

Tests performed in addition to those selected for level 7 and the parameters I selected are:

Test	Default Parameter	New Parameter
non-default accounts in DBA role	N/A	N/A
number of users logged on in DBA role at time of scan	3	1
login encryption setting	N/A	N/A
OS Authentication prefix	OPS$	“”
Password Grace Time	10	10
Password Life Time	45	90
Password Lock Time	5	1

Password Reuse Max		5	12
Password Verify Function		VERIFY_FUNCTION	NULL
Role Passwords		N/A	N/A
Audit Table Permissions		NULL	SYS, SYSTEM, AUDITOR
Logon Hours Violations		Sun-Sat 6-11	Mon-Fri 9-5
Audit Trail		N/A	N/A
Auditing of commands	None	CREATE SESSION BY SESSION WHEN [UN]SUCCESSFUL CREATE/ALTER/DROP USER BY ACCESS WHEN [UN]SUCCESSFUL BECOME USER BY ACCESS WHEN [UN]SUCCESSFUL	
Auditing of schema objects		N/A	N/A
Composite Resource Usage		1000000	1000000
Concurrent Sessions Resource Usage Limit		1	1
Connect Time Resource Usage Limit		90	90
CPU/Call Resource Usage Limit		100000	100000
CPU/Session resource Usage Limit		1000000	1000000
Idle Time Resource Usage Limit		15	20
Oracle Licensing Compliance		N/A	N/A
Oracle SQL_02 SECURITY		N/A	N/A
Oracle Wallet permissions		750	WinNT N/A
Password Verify Function Changes		N/A	N/A
Private SGA Resource Usage Limit		256	256
Reads/Call Resource Usage Limit		5000	5000
Reads/Session Resource Usage Limit		50000	50000
Resource Limits Not Enabled		N/A	N/A

I logged on as user SYSTEM using SQL*Plus. The tests, commands, results and compliance are listed below.

Brief Test Description	Command and results	Compliant?
Account Permissions	SQL> select grantee,granted_role from dba_role_privs where granted_role='DBA'; GRANTEE GRANTED_ROLE ------------------------------ ------------------------------ SYS DBA SYSTEM DBA	Y
Audit Table Permissions	SQL> select * from user_tab_privs where table_name ='AUD$'; no rows selected	Y

Audit Table Tablespace	SQL> select tablespace_name from dba_tables where table_name='AUD$'; TABLESPACE_NAME ------------------------------ SYSTEM	N
Audit Trail Location	View init.ora #audit_trail = true # if you want auditing no entry for audit_file_dest	N
Auditing of Commands	SQL> select * from dba_priv_audit_opts where privilege = 'CREATE SESSION'; no rows selected SQL> select * from dba_priv_audit_opts where privilege = 'CREATE USER'; no rows selected SQL> select * from dba_priv_audit_opts where privilege = 'ALTER USER'; no rows selected SQL> select * from dba_priv_audit_opts where privilege = 'DROP USER'; no rows selected SQL> select * from dba_priv_audit_opts where privilege = 'BECOME USER'; no rows selected	N
Composite Resource Usage Limit	SQL> select profile,limit from dba_profiles where resource_name ='COMPOSITE_LIMIT'; PROFILE LIMIT ------------------------------ ---------- DEFAULT UNLIMITED	N
Concurrent Sessions Resource Usage Limit	SQL> select profile,limit from dba_profiles where resource_name ='SESSIONS_PER_USER'; PROFILE LIMIT ------------------------------ ---------- DEFAULT UNLIMITED	N
Connect Time Resource Usage Limit	SQL> select profile,limit from dba_profiles where resource_name ='CONNECT_TIME'; PROFILE LIMIT ------------------------------ ---------- DEFAULT UNLIMITED	N
CPU/Call Resource Usage Limit	SQL> select profile,limit from dba_profiles where resource_name ='CPU_PER_CALL'; PROFILE LIMIT ------------------------------ ---------- DEFAULT UNLIMITED	N

CPU/Session Resource Usage Limit	SQL> select profile,limit from dba_profiles where resource_name ='CPU_PER_SESSION'; PROFILE LIMIT ------------------------------ ---------- DEFAULT UNLIMITED	N
Data Dictionary Accessibility	SQL> show parameters NAME TYPE VALUE ------------------------------------ ------- ------------------------------ O7_DICTIONARY_ACCESSIBILITY boolean TRUE	Y
Database Link Password Encryption	SQL> show parameters NAME TYPE VALUE ------------------------------------ ------- ------------------------------ dblink_encrypt_login boolean FALSE	N
Database Link Password Unencrypted	SQL> select PASSWORD,AUTHPWD from SYS.LINK$; no rows selected	Y
Database Link Permissions	SQL> select * from dba_tab_privs where owner='SYS' and TABLE_NAME='LINK$'; no rows selected	Y
DBA Includes Non-default Account	SQL> select grantee, granted_role from dba_role_privs where granted_role='DBA'; GRANTEE GRANTED_ROLE ------------------------------ ------------------------------ SYS DBA SYSTEM DBA SQL> select * from role_role_privs where granted_role='DBA'; no rows selected	Y
Default Accounts and Passwords	SQL> select username from all_users; USERNAME ------------------------------ SYS SYSTEM OUTLN DBSNMP SQL> connect sys/change_on_install Connected. SQL> connect system/manager Connected. SQL> connect outln/outln Connected. SQL>	N
Default Internal Password	SQL> connect internal Connected. SQL>	N

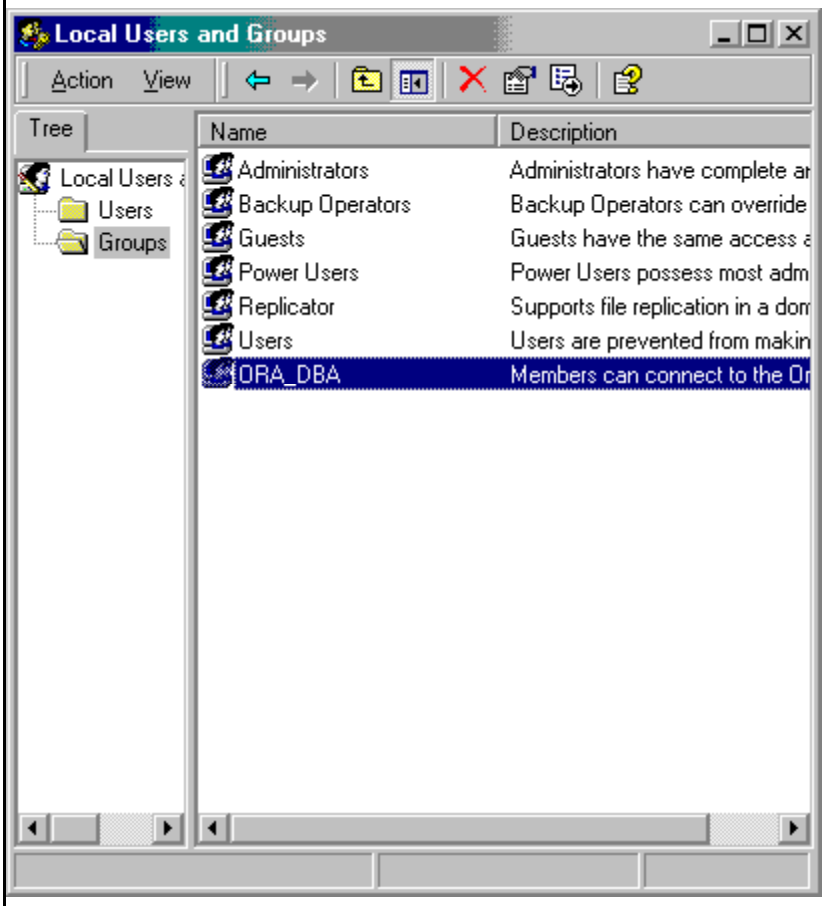
Default Listener Password	<ENTER> means Enter key pressed without entering text. LSNRCTL> change_password Old password:<ENTER> New password:<ENTER> Reenter new password:<ENTER> Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=k62)(PORT=1521))) Password changed for LISTENER The command completed successfully LSNRCTL>	N
Default Password Verify Function	Using information in the comments in ISS Database Scanner I have assumed that this test: SQL>COLUMN text format A255 SQL> select TEXT from dba_source where name='VERIFY_FUNCTION' order by LINE; no rows selected The default password checking function does not exist. If it did it could be compared to UTLPWDMG.SQL and recreated using the same script.	N
Default SAP Account and Password	SQL> connect sap/sapr3 ERROR: ORA-01017: invalid username/password; logon denied	Y
Default SNMP Account	SQL> connect dbsnmp/dbsnmp Connected.	N
Default Tablespace	SQL> select username,default_tablespace from dba_users; USERNAME DEFAULT_TABLESPACE ------------------------------ ------------------------------ SYS SYSTEM SYSTEM TOOLS OUTLN SYSTEM DBSNMP SYSTEM	N
Excessive DBA Connections	COULD NOT FIND THIS INFORMATION	?
Expired Passwords Found in Oracle 8	SQL> select profile,limit from dba_profiles where resource_name='PASSWORD_LIFE_TIME'; PROFILE LIMIT ------------------------------ ---------- DEFAULT UNLIMITED	N
Failed Login Attempts	SQL> select profile,limit from dba_profiles where resource_name='FAILED_LOGIN_ATTEMPTS'; PROFILE LIMIT ------------------------------ ----------- DEFAULT UNLIMITED	N

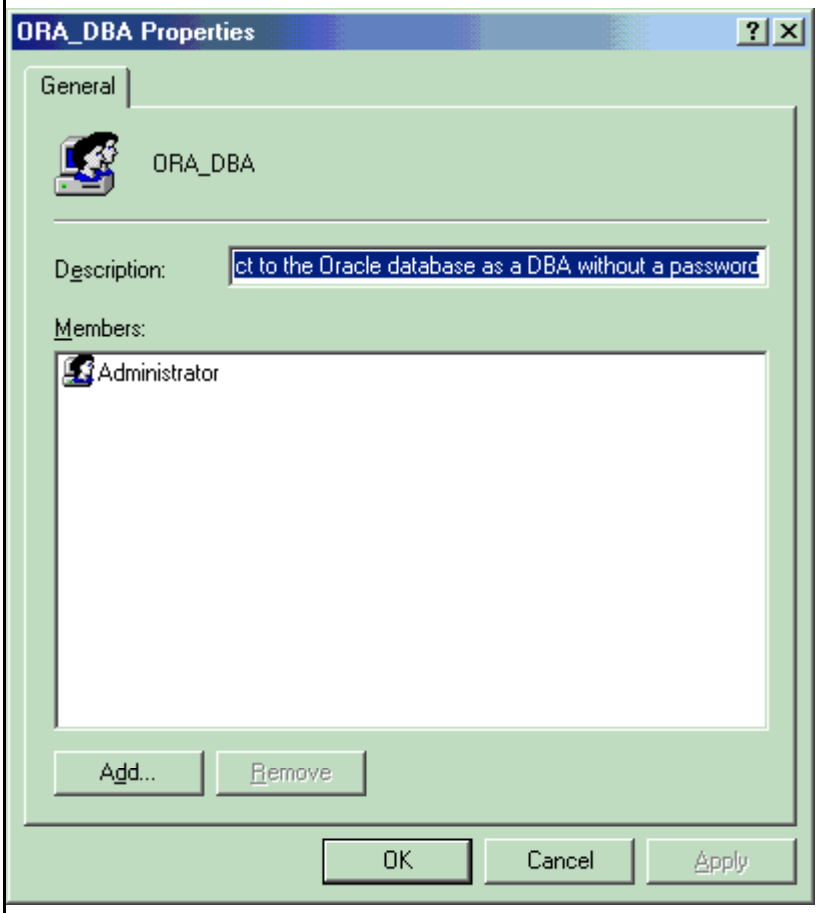
File Checksums	Information from previous scan not available. Run versioner-06b.exe or Winterrogate on <ORACLE_HOME> Output file versioner_output.csv http://winfingerprint.sourceforge.net/	Y
File Group	INSTALLED ON FAT PARTITION SO ACLs NOT AVAILABLE Information from previous scan not available. Run DUMPSEC http://www.somarsoft.com/ Output File dumpsec_file_perm_output.txt	N
File Modifications	Information from previous scan not available. Run versioner-06b.exe or Winterrogate on <ORACLE_HOME> Output file versioner_output.csv Http://winfingerprint.sourceforge.net/	Y
File Owner	INSTALLED ON FAT PARTITION SO ACLs NOT AVAILABLE Information from previous scan not available. Run DUMPSEC http://www.somarsoft.com/ Output File dumpsec_file_perm_output.txt	N
File Permissions	INSTALLED ON FAT PARTITION SO ACLs NOT AVAILABLE Information from previous scan not available. Run DUMPSEC http://www.somarsoft.com/ Output File dumpsec_file_perm_output.txt	N
File Permissions – listener.ora	Cacls listener.ora INSTALLED ON FAT PARTITION – NO ACLs POSSIBLE	N
File Permissions - snmp file	Cacls snmp.ora Cacls snmp_rw.ora INSTALLED ON FAT PARTITION – NO ACLs POSSIBLE Also NOT INSTALLED ON THIS SYSTEM	Y
File Permissions - SYSDBA password file	Cacls PWDorcl.ora INSTALLED ON FAT PARTITION – NO ACLs POSSIBLE	N
Idle Time Resource Usage Limit	SQL> select profile,limit from dba_profiles where resource_name='IDLE_TIME'; PROFILE LIMIT ---------- ---------- DEFAULT UNLIMITED	N
Intelligent Agent Patch	COULD NOT FIND THIS INFORMATION	?
Internal Password in Spoolmain	View spoolmain.log file. FILE NOT FOUND ON THIS SYSTEM	Y

Listener Cleartext Password	View listener.ora No Passwords stored	Y
Login Encryption Setting	View AUTOEXEC.BAT No line containing SET ORA_ENCRYPT_LOGIN=TRUE	N
Logon Hours Violations	SQL> select username from dba_audit_session 2 where (to_number(to_char(timestamp,'HH24')) < 9) 3 or (to_number(to_char(timestamp,'HH24')) > 17) 4 or (to_number(to_char(timestamp,'D')) = 1) 5 or or (to_number(to_char(timestamp,'D')) = 7); no rows selected	Y
Oracle Licensing Compliance	SQL> show parameters NAME TYPE VALUE ---------- ------- ----- license_max_sessions integer 0 license_max_users integer 0	N
Oracle SQL92_SECURITY	NAME TYPE VALUE ---------- ------- ----- sql92_security boolean FALSE	N
Oracle Wallet Permissions	Cacls sqlnet.ora INSTALLED ON FAT PARTITION - NO ACLs POSSIBLE	N
OS Authentication Prefix	NAME TYPE VALUE ---------- ------- ------ os_authent_prefix string	Y
Password Attacks	SQL> select * from dba_priv_audit_opts where privilege = 'CREATE SESSION'; no rows selected	N
Password Grace Time	SQL> select profile,limit from dba_profiles where resource_name ='PASSWORD_GRACE_TIME'; PROFILE LIMIT ---------- ---------- DEFAULT UNLIMITED	N
Password Life Time	SQL> select profile,limit from dba_profiles where resource_name ='PASSWORD_LIFE_TIME'; PROFILE LIMIT ---------- ---------- DEFAULT UNLIMITED	N
Password Lock Time	SQL> select profile,limit from dba_profiles where resource_name ='PASSWORD_LOCK_TIME'; PROFILE LIMIT ---------- ---------- DEFAULT UNLIMITED	N

Password Reuse Max	SQL> select profile,limit from dba_profiles where resource_name ='PASSWORD_REUSE_MAX'; PROFILE LIMIT ------------------------------ ---------- DEFAULT UNLIMITED	N
Password Reuse Time	SQL> select profile,limit from dba_profiles where resource_name ='PASSWORD_REUSE_TIME'; PROFILE LIMIT ------------------------------ ---------- DEFAULT UNLIMITED	N
Password Verify Function Set Properly	SQL> select profile,limit from dba_profiles where resource_name ='PASSWORD_VERIFY_FUNCTION'; PROFILE LIMIT ------------------------------ ---------- DEFAULT UNLIMITED	N
Password Verify Function Changes	Using information in the comments in ISS Database Scanner I have assumed that this test: SQL> select resource_name,limit from dba_profiles where resource_name=’ PASSWORD_VERIFY_FUNCTION’; RESOURCE_NAME LIMIT ------------------------------ ---------- PASSWORD_VERIFY_FUNCTION UNLIMITED No extra password checking functions are to be used. If the default ‘verify_function’ was enabled the source in DBA_SOURCE could be compared to the original in UTLPWDMG.SQL and recreated using the same script. If a custom function was enabled the source in DBA_SOURCE could only be checked by comparing a copy of the source extracted during a previous scan.	N
Private SGA Resource Usage Limit	SQL> select profile,limit from dba_profiles where resource_name ='PRIVATE_SGA'; PROFILE LIMIT ------------------------------ ---------- DEFAULT UNLIMITED	N

Privileged OS Users	Check in appropriate User manager application for groups ORA_<sid>_DBA, ORA_<sid>_OPER, ORA_DBA, and ORA_OPER and see who are members.	





Privileges Granted With Admin	SQL> select * from dba_sys_privs where ADMIN_OPTION='YES' and GRANTEE not in ('DBA','SYS','SYSTEM'); GRANTEE PRIVILEGE ADM ---------- ---------- --- AQ_ADMINISTRATOR_ROLE DEQUEUE ANY QUEUE YES AQ_ADMINISTRATOR_ROLE ENQUEUE ANY QUEUE YES AQ_ADMINISTRATOR_ROLE MANAGE ANY QUEUE YES	N
PUBLIC Object Permissions	SQL> select table_name,privilege from dba_tab_privs where grantee='PUBLIC'; .. .. .. 598 rows selected. SQL> select table_name,privilege from dba_tab_privs where grantee='PUBLIC' and owner <> 'SYS'; TABLE_NAME PRIVILEGE ---------- --------- PRODUCT_PRIVS SELECT SQL> select table_name,privilege from dba_tab_privs where grantee='PUBLIC' and PRIVILEGE not in ('EXECUTE','SELECT'); TABLE_NAME PRIVILEGE ---------- --------- PSTUBTBL DELETE	?
PUBLIC System Privileges	SQL> select * from dba_sys_privs where grantee='PUBLIC'; no rows selected	Y
Reads/Call Resource Usage Limit	SQL> select profile,limit from dba_profiles where resource_name ='LOGICAL_READS_PER_CALL'; PROFILE LIMIT ---------- ---------- DEFAULT UNLIMITED	N
Reads/Session Resource Use Limit	SQL> select profile,limit from dba_profiles where resource_name ='LOGICAL_READS_PER_SESSION'; PROFILE LIMIT ---------- ---------- DEFAULT UNLIMITED	N
Registry Permissions	Run DUMPSEC http://www.somarsoft.com/ Output File dumpsec_rep_perm_output.txt	?
Remote Login Password File	SQL> show parameters NAME TYPE VALUE ---------- ---------- --------- remote_login_passwordfile string EXCLUSIVE	N
Resource Limits Not Enabled	SQL> show parameters NAME TYPE VALUE ---------- ---------- --------- resource_limit boolean FALSE	N

Role Passwords	SQL> select * from dba_roles; ROLE PASSWORD ------------------------------ -------- CONNECT NO RESOURCE NO DBA NO SELECT_CATALOG_ROLE NO EXECUTE_CATALOG_ROLE NO DELETE_CATALOG_ROLE NO EXP_FULL_DATABASE NO IMP_FULL_DATABASE NO RECOVERY_CATALOG_OWNER NO AQ_ADMINISTRATOR_ROLE NO AQ_USER_ROLE NO ROLE PASSWORD ------------------------------ -------- SNMPAGENT NO OEM_MONITOR NO HS_ADMIN_ROLE NO 14 rows selected.	Y
Role Permissions	Using information in the comments in ISS Database Scanner I have assumed that this test: SQL> select grantee,table_name from dba_tab_privs where grantee not in ('DBA','SYS','SYSTEM') 2 and table_name in (select object_name from dba_objects where object_type='TABLE'); GRANTEE TABLE_NAME ------------------------------ ---------------------- AQ_ADMINISTRATOR_ROLE AQ$_PROPAGATION_STATUS DELETE_CATALOG_ROLE AUD$ PUBLIC AUDIT_ACTIONS PUBLIC DUAL EXP_FULL_DATABASE INCEXP EXP_FULL_DATABASE INCEXP EXP_FULL_DATABASE INCEXP EXP_FULL_DATABASE INCFIL EXP_FULL_DATABASE INCFIL EXP_FULL_DATABASE INCFIL EXP_FULL_DATABASE INCVID GRANTEE TABLE_NAME ------------------------------ ---------------------- EXP_FULL_DATABASE INCVID EXP_FULL_DATABASE INCVID PUBLIC PSTUBTBL PUBLIC PSTUBTBL PUBLIC STMT_AUDIT_OPTION_MAP PUBLIC SYSTEM_PRIVILEGE_MAP PUBLIC TABLE_PRIVILEGE_MAP 18 rows selected.	N

Roles Granted With Admin	SQL> select * from dba_role_privs where ADMIN_OPTION='YES' and GRANTEE not in ('DBA','SYS','SYSTEM') ; no rows selected	Y
Stale Accounts	SQL> select username from dba_users where username not in 2 (select username from dba_audit_session where timestamp > SYSDATE -30); USERNAME ------------------------------ SYS SYSTEM OUTLN DBSNMP Stale Oracle accounts found by looking for logon records in audit table. Assumes audit is turned on and each account has at least one logon.	Y
Trusting Remote OS Authenticati on Setting	SQL> show parameters NAME TYPE VALUE ------------------------------------ ------- ----- .. remote_os_authent boolean FALSE	Y
Trusting Remote OS for Roles Setting	SQL> show parameters NAME TYPE VALUE ------------------------------------ ------- ----- .. remote_os_roles boolean FALSE	Y
Unencrypted SNMP Password	View files snmp.ora and snmp_rw.ora FILES NOT FOUND ON THIS SYSTEM.	Y
Use of CONNECT Default Role	SQL> select * from dba_role_privs where granted_role='CONNECT'; GRANTEE GRANTED_ROLE ADM DEF ------------------------------ ------------ --- --- DBSNMP CONNECT NO YES OEM_MONITOR CONNECT NO YES OUTLN CONNECT NO YES SYS CONNECT YES YES	N
Use of RESOURCE Default Role	SQL> select * from dba_role_privs where granted_role='RESOURCE'; GRANTEE GRANTED_ROLE ADM DEF ------------------------------ ------------ --- --- DBSNMP RESOURCE NO YES OUTLN RESOURCE NO YES SYS RESOURCE YES YES	N
UTL_FILE Permissions	SQL> select grantee,privilege from dba_tab_privs where table_name='UTL_FILE'; GRANTEE PRIVILEGE ------------------------------ --------- PUBLIC EXECUTE	N

UTL_FILE_DIR Setting	SQL> show parameters NAME TYPE VALUE ------------------------------------ ------- ----- utl_file_dir string	Y
View Missing With Check Option	SQL> select TEXT from dba_views where view_name in 2 (select table_name from dba_tab_privs where privilege in ('INSERT','UPDATE') and table_name in 3 (select object_name from dba_objects where object_type='VIEW')); no rows selected If rows are selected the WITH CHECK option must appear at the end of every text field.	Y
With Grant Option	SQL> select grantee,table_name from dba_tab_privs where GRANTABLE='YES' and grantee not in 2 ('DBA','SYS','SYSTEM'); .. .. 272 rows selected. SQL> select grantee,table_name from dba_tab_privs where GRANTABLE='YES' and grantee not in('DBA','SY S','SYSTEM','PUBLIC'); no rows selected	N

Subjective Tests

Test	Non-Compliant if …	External Written Policy Required

Audit Trail	Could just select whole audit trail but this looks for actions that should be performed by an administrator. First check for non-admins doing these actions then see what the administrator users have been up to. SQL> select username,action_name,obj_name from dba_audit_trail where 2 username not in ('DBA','SYS','SYSTEM') 3 and 4 (action_name like '%CREATE%' 5 or action_name like '%DROP%' 6 or action_name like '%ALTER%' 7 or action_name like '%GRANT%' 8 or action_name like '%AUDIT%' 9 or action_name like '%REVOKE%'); no rows selected SQL> select username,action_name,obj_name from dba_audit_trail where 2 action_name like '%CREATE%' 3 or action_name like '%DROP%' 4 or action_name like '%ALTER%' 5 or action_name like '%GRANT%' 6 or action_name like '%AUDIT%' 7 or action_name like '%REVOKE%'; no rows selected	Y

Auditing of Schema Objects	SQL> select count(*) from dba_obj_audit_opts; COUNT(*) ---------- 1682 SQL> select * from dba_obj_audit_opts where 2 ALT <> '-/-' or 3 AUD <> '-/-' or 4 COM <> '-/-' or 5 DEL <> '-/-' or 6 GRA <> '-/-' or 7 IND <> '-/-' or 8 INS <> '-/-' or 9 LOC <> '-/-' or 10 REN <> '-/-' or 11 SEL <> '-/-' or 12 UPD <> '-/-' or 13 REF <> '-/-' or 14 EXE <> '-/-' or 15 CRE <> '-/-' or 16 REA <> '-/-' or 17 WRI <> '-/-'; no rows selected These audit configuration options are usually kept to a minimum so the list returned by the above statement should be short enough to check by hand.	Y

Evaluation of the Audit

The audit is thorough and the Database Scanner software is widely configurable. It would take some time to be proficient with all the options. There is a large volume of data to sift through when all tests are run and it can be difficult to correlate significant pairs of results. If a clear-text password is stored in listener.ora then the file permissions on this file should be checked. This is particularly true of the actual output from Database Scanner where there are 21 reports to choose from. Overall the Database Scanner checks the security of the system well and it is a valuable addition to a manual audit.

The checks on Authentication issues are good and all points where there is an impact on secure access to the system seem to be checked. It covers the obvious security holes of default passwords and paswords with poor security, such as long lifetime. Although brute force password check is untested this would be very useful. The checks on Authorization to use system resources are sufficient with check on PUBLIC grants and GRANTS with ADMIN rights. One omission is a check for roles granted to PUBLIC. The checks to make sure Table data is only accessed through Views or synonyms are particularly useful. The System Integrity checking caters much more for Unix looking for setuid and setgid files

although all the resource usage limit checks are applicable across all platforms. The file integrity checking is probably best left to an external tool like Tripwire – it is unclear what checksum algorithm is used.

The biggest omission is checking for software vulnerabilities, except for one check for the Intelligent Agent patch. This is an unacceptable flaw in the software and would have to be compensated for with a manual check. The software needs updating to take account of changes in Oracle software especially the newer UTL packages. Network accessibility is weak and while some of this could be said to sit better in the Internet Scanner product the Net8 IP filtering should be tested by this software. The package should check user schemas for objects, with a parameter to exclude application code owner usernames. This would help avoid data manipulation attacks. Use of PLSQL+WRAP should be checked as this can slow down attackers and hide important information.

I was unable to check who was logged on using DBA privilege at the time of the scan. Further research should yield a solution to this query. I could not formulate a test to see if the Intelligent Agent Patch was installed – except to say that I haven't installed it. Again a test should be possible with further research.

Directions for future work

This audit needs to be done on an Oracle 7.1.6 system with all the latest patches installed and the software placed on an NTFS volume to produce the definitive results. The software needs to be checked against an Oracle 9.0 database to see if there are any significant differences.

Suggestions for extra tests are listed in the section near the start of this document called "Why Current Methods and Techniques Need Improvement". The software is not easily extensible with a scripting language like Nessus. Extra tests would need to be included by the manufacturer or processed using an external SQL script. The examples given in this document show that acquiring the correct data is not difficult.

All areas of the audit are well defined apart from those referring to the PASSWORD_VERIFY_FUNCTION – "Password Verify Function", "Default Password Verify Function" and "Password Verify Function Changes". These tests are phrased in a confusing fashion. After re-reading the three tests several times I now understand what they are testing.

The efficiency of the audit could be improved by allowing filtering of the audit trail by date and allowing significant audit events to be selected instead of the whole audit trail being dumped to file. With logon and logoff audit enabled this report would be huge.

Intellectual property issues permitting this audit evaluation exercise needs to be turned into a free audit tool. This will probably require starting from scratch using SQL scripts.

The following tools should be investigated to see if they apply to Oracle databases [13]:

Audit Command Language (ACL)
CAATs
ENTACT
Kaplan's Auditnet Resources
Horwarth Software Co. (UK)
SARA
Auditor Assistant
Oracle Tools for change mgmt and real-time monitoring of Oracle Applications
Audimation Services, IDEA
Methodware, COBIT Advisor

References

1. Theriault, Marlene, and William Heney, Oracle Security, Sebastopol CA: O'Reilly & Associates, Inc., 1998.

2. Smith, Howard, "Hack Proofing Oracle", Oracle Corporation UK Limited, URL: http://otn.oracle.com/deploy/security/pdf/oow00/orahack.pdf (13 May 2001).

3. Paul Haigh, "Oracle Database HOWTO v1.2, 4 August 1998", URL: http://ldp.dgc-nms.co.uk/ldp/HOWTO/Oracle-7-HOWTO.html

4. Stephen Darlington, "Oracle for Linux Installation HOWTO 1.14 2000/06/19 1:07:43" URL: http://ldp.dgc-nms.co.uk/ldp/HOWTO/Oracle-8-HOWTO.html

5. Nessus. "Introduction." URL: http://www.nessus.org/ (21 August, 2001)

6. Nessus: "Nessus Security Checks." URL: http://cgi.nessus.org/plugins/dump.php3, (21 August, 2001)

7. "Oracle 8i Concepts" Controlling Database Access, URL: http://technet.oracle.com/docs/products/oracle8i/doc_library/817_doc/server.817/a76965/toc.htm

8. "Oracle 8i Administrator's Guide" Controlling Database Access, URL: http://technet.oracle.com/docs/products/oracle8i/doc_library/817_doc/server.817/a76956/toc.htm

9. Internet Security Systems, "Securing Database Servers" URL: http://documents.iss.net/whitepapers/securingdbs.pdf

10. Internet Security System, Database Scanner – Getting Started, Version 4.1, Jan 2001, URL: http://documents.iss.net/literature/DatabaseScanner/DBS41_ug.pdf

11. Internet Security Systems Database Scanner, "OracleVulns Access Database table", C:\Program Files\ISS\DBScan40\Setup.mdb

12. Internet Security System, Xpress Updates, URL: https://www.iss.net/cgi-bin/download/evaluation/download_product.cgi Accessible by navigation from top page to product downloads, the filling in registration page.

13. The Information Systems Audit and Control Association & Foundation, "KNET", URL: http://www.isaca.org/gir/girMenu.cfm

Bibliography

Lorraina Hazel, CNE, "An Overview of Oracle Database Security Features"
URL: http://www.sans.org/infosecFAQ/appsec/oracle.htm (May 13, 2001).

1. "Database Security In Oracle8i" An Oracle Technical White Paper, November 1999,
URL: http://technet.oracle.com/deploy/security/pdf/oow99/dbswp86.pdf (13 May 2001).

2. "Untitled", An Oracle 8i Overview,
URL:http://technet.oracle.com/deploy/security/oracle8i/htdocs/overview.htm (13 May 2001).

4. Koch, George, and Kevin Loney, Oracle8: The Complete Reference, Berkely CA: Osborne McGraw-Hill,
1997.

5. Kreines, David C., and Brian Laskey, Oracle Database Administration, Sebastopol CA: O'Reilly &
Associates, Inc., April 1999.

6. "Meeting the Availability Needs of the Mission-Critical Enterprise with Oracle8i" An Oracle Business
White Paper, February 1999,
URL:http://www.oracle.com/collateral/o8i_high_avail_enhance_fo.pdf (13 May 2001).

7. Smith, Howard, "Hack Proofing Oracle", Oracle Corporation UK Limited,
URL: http://otn.oracle.com/deploy/security/pdf/oow00/orahack.pdf (13 May 2001).

8. "Computer Security Criteria: Security Evaluations and Assessment" An Oracle White Paper, October
2000,
URL: http://www.oracle.com/ip/solve/security/seceval_wp.pdf (13 May 2001).

9. "Introduction to Oracle Advanced Security", Oracle Advanced Security Administrator's Guide, Release
8.1.5,
URL: http://technet.oracle.com/doc/network.815/a67766/toc.htm (13 May 2001).

10. "Oracle 8i Release 3 New Features Summary" Features Overview, August 2000,
URL: http://technet.oracle.com/products/oracle8i/pdf/8iR3_nfs.pdf (13 May 2001).

11. "Oracle 8i Concepts" Controlling Database Access,
URL:
http://technet.oracle.com/docs/products/oracle8i/doc_library/817_doc/server.817/a76965/c25acces.htm (13 May 2001).

Carmichael, Paul, "Securing Databases"
URL: http://www.sans.org/infosecFAQ/appsec/database.htm (April 9, 2001)

BrainTree Security Software, Security at the Heart of B2B E-Transactions, 1999, http://www.sqlsecure.com/Whitepapers/3-Tier_Data_Security/WP_Download/bti_down2/B2bwp.pdf (3rd April, 2001)

BrainTree Security Software, Securing PeopleSoft ?Data, http://www.sqlsecure.com/Whitepapers/3-Tier_Data_Security/WP_Download/bti_down2/Pswp.pdf (3rd April, 2001)

BrainTree Security Software, Client/Server Database Security, http://www.sqlsecure.com/Whitepapers/3-Tier_Data_Security/WP_Download/bti_down2/Cswp.pdf (3rd April, 2001)

Oracle, Database Security in Oracle8i, An Oracle Technical White Paper, November 1999, URL http://technet.oracle.com/deploy/security/seceval/pdf/seceval_wp.pdf (3rd April, 2001)

Yeo, Lisa. "Configuring and Auditing Windows NT with Security Configuration Manager." September 2000. URL: http://www.sans.org/giactc/gcnt.htm (23 March 2001).

Toy, Steven. "Centralized Auditing of a Windows NT Computer." URL: http://www.sans.org/giactc/gcnt.htm (23 March 2001).

Carboni, Christopher. "Christopher_Carboni.doc." URL: http://www.sans.org/giactc/gcnt.htm (23 March 2001).

Jain, Anil K. "Developments in Auditing NT." URL: http://www.sans.org/giactc/gcnt.htm (23 March 2001).