

60 Security Tips

60
MINUTES



60 Oracle Security Tips in 60 Minutes

SEOUC 2007

Kenny Smith

(and Trish Holliman, Igor Ryzhkov & Bob
Vance)

Cnetics
www.cnetics.com

Understand Exploits

- **What:** Oracle exploits are available for review and experimentation
- **Why:** Understanding and demonstrating exploits can raise data security awareness
- **How:** Find exploit information and play with hacks on test databases
- **Where:**
 - Aaron Neuman’s “Anatomy of a Database Attack”
 - Review www.red-database-security.com site
 - Badstore.net, CAIN, password crackers

Hijack a User's Account

- **What:** A user's password hash can be captured from DBA_USERS or export file. Someone with ALTER USER privilege can change the password, do some work, then replace the password using the hash
- **Why:** Misuse can occur as a trusted user without that user's detection
- **Where:** See
 - www.pentest.co.uk/documents/ora_pwd_thorts.htm
 - <http://asktom.oracle.com> for "Password in DBA_USERS"

Hijack a User's Account

```
SELECT password FROM dba_users WHERE  
  username = 'SCOTT';  
ALTER USER scott IDENTIFIED BY hijack;  
CONNECT scott/hijack  
GRANT SELECT ON scott.emp to PUBLIC  
ALTER USER scott IDENTIFIED BY VALUES  
  '23E3F8C1BB14BB4D';
```

Hijack a User's Account

- To prevent and detect this attack:
 - ❑ Limit user access to the DBA_USERS view
 - ❑ Audit database changes like user password alterations or escalation of privileges
 - ❑ Prevent commands by being run via PRODUCT_USER_PROFILE table entries.

Automate Database Assessments

- **What:** Examine your database for vulnerabilities
- **Why:** Helps you catch problems
- **How:** Automated options include:
 - Oracle Enterprise Manager (Configuration Pack)
 - Application Security's AppDetective
 - Center for Internet Security Benchmarking tool
- **Where:** See these sites
 - www.oracle.com/technology/products/oem/pdf/ds_as_cmp_r2.pdf
 - www.appsecinc.com
 - www.cisecurity.org
- **Note:** Find databases with Nessus or AppDetective

Install with Limited Product Options

- **What:** Oracle Software is rich with product features (Spatial, UltraSearch, Context, Apache)
- **Why:** Limit attack/misuse surface area
- **How:** Choose only needed options on Oracle Universal (OUI) Installer & Database Configuration Assistant (dbca)
- **Where:** See product install guides



Lock Down Default Users

- **What:** Oracle provides default users with database and product options, which allow others to gain access to systems.
- **Why:** Well known and open default users provide access for misuse.
- **How:** Check for default user passwords by
 - Download patch #4926128 from the Oracle Website and run script
 - Download a free password checker from www.red-database-security.com
 - Purchase Application Security's AppDetective
- **Where:**
 - www.red-database-security.com/whitepaper/oracle_passwords.html
 - www.petefinnigan.com/default/default_password_list.htm

Control Application Connection at Logon

- **What:** Use a logon trigger to control which users access a database system
- **Why:** Keep staff from using TOAD, Excel, Access ... from accessing production system
- **Where:** See code on next slide

Control Application Connection at Logon (How)

```
CREATE OR REPLACE TRIGGER check_session_connection
AFTER LOGON ON DATABASE
DECLARE
  cursor c_session is
    select sys_context('userenv','session_user') username,
           s.module, s.program
    from v$session s
    where sys_context('userenv','sessionid')=s.audsid;
  r_session c_session%rowtype;
BEGIN
  OPEN c_session;
  FETCH c_session into r_session;
  IF upper(r_session.module) like ('%EXCEL%') THEN
    raise_application_error (20901,'Excel - go away. ');
  END IF;
  IF upper(r_session.module) like ('%ACCESS%') THEN
    raise_application_error (20902,'Access - go away. ');
  END IF;
  CLOSE c_session;
END;
```

Remove Extra Database Accounts

- **What:** Product options often require schemas. These accounts can often be removed or should be locked if not used
- **Why:** Limit the misuse “surface area”
- **How:** Unneeded accounts can be either removed or locked according to Metalink notes.
- **Where:** See Metalink notes in table...

Remove Extra Database Accounts (Examples)

User	Password	Notes	Removal
DBSNMP	DBSNMP	Oracle Agent	@?/rdbms/admin/catnsnmp.sql
DMSYS	DMSYS	Oracle data mining	Metalink Note:297551.1
MDSYS	MDSYS	Spatial Data Option	Metalink Note:179472.1
ORDSYS	ORDSYS	InterMedia Audio option	@?/ord/im/admin/imdtyp.sql
OULTN	OULTN	Stored Outlines	Cannot be dropped, only locked. Metalink Note: 160861.1

Hide Password Hashes from Outsiders

- **What:** Oracle stores passwords as hashes. With hash value, passwords can be reverse engineered.
- **Why:** With password cracking program, hackers can break password given the hash.
- **How:**
 - Force password complexity (password verification function)
 - Require frequent password changes
 - Limit access to dictionary tables with password hash values (DBA_USERS, SYS.USER\$, SYS.USER_HISTORY\$)
 - Consider Oracle's Advanced Security Option
 - for Oracle Net traffic encryption
 - for alternative user authentication
 - Turn on auditing for access to the DBA_USERS view.
- **Where:** Review SANS paper & Oracle response
 - SANS - "An Assessment of the Oracle Password Hashing Algorithm," www.sans.org/rr/special/index.php?id=oracle_pass.
 - Oracle's response on Metalink (Note:340240.1)



Force Complex Passwords

- **What:** Oracle allows easy password creation without mixed case or special characters. You can force Oracle to check the complexity of a password when set using a password verification function attached to a profile
- **Why:** Users will set easy to remember passwords unless complexity is forced upon them
- **How:** Use the Oracle supplied password verification like this or create your own.

```
SQL> @?/rdbms/admin/utlpwdmg.sql  
SQL> alter profile default limit  
password_verify_function verify_function;
```

- **Where:** Oracle Database Security Guide 10g Release 2 (10.2) Section 7.4

Hide the Database Link Passwords

- **What:** Prior to version 10g Release 2, Oracle stored user name and password information for fixed user database links in data dictionary views. The password was in clear text
- **Why:** Anyone with access to this view could see the username and password combination and connect string
- **How:** Protect the access to other systems:
 - Confirm that SYS.LINK\$ is not selectable from public
 - Take steps to remove data dictionary access from users
 - Create CURRENT_USER links if possible
 - Limit users capability to create database links
 - Check that links in the database are used
 - Consider remote database link authentication (Kerberos)
- **Where:** Oracle Database SQL Reference “CREATE DATABASE LINK”

Manage Password Changes with User Profiles

- **What:** Managing the lifetime and reuse policies of an Oracle database can be done by with Oracle user profiles. Six profile limits dictate password aging, reuse and locking.
- **Why:** Prevent brute force attacks and keep users from reusing passwords.

Profile Limit	Defined
FAILED_LOGIN_ATTEMPTS	failed attempts to log in
PASSWORD_LIFE_TIME	days the same password can be used for authentication
PASSWORD_REUSE_TIME	days before which a password cannot be reused
PASSWORD_REUSE_MAX	passwords required before reuse
PASSWORD_LOCK_TIME	days an account will be locked after failed login attempts
PASSWORD_GRACE_TIME	days after the grace period begins

Manage Password Changes with User Profiles (...)

- Allow 2 sessions per user
- Lock account after 3 consecutive failed attempts
- Expire passwords after 90 days
- Prevent password reuse for 1 year
- Prevent password reuse until 20 changes
- Lock accounts for 1 minute on failed attempts
- Warn 3 days for users to change password

```
ALTER PROFILE DEFAULT LIMIT
SESSIONS_PER_USER          2
FAILED_LOGIN_ATTEMPTS     3
PASSWORD_LIFE_TIME        90
PASSWORD_REUSE_TIME       365
PASSWORD_REUSE_MAX        20
PASSWORD_LOCK_TIME        .0006
PASSWORD_GRACE_TIME       3;
```

Keep Passwords off Command Line

- **What:** Oracle automated processes require authentication. Insure that username/passwords aren't easily captured from process lists
- **Why:** Anyone with access to process listing may see connection credentials
- **How:** Check that...
 - username and password are not command line arguments for tools
 - SQL*Plus – use a “here” document or command file
 - For RMAN, export and import, use parameter or command files as input
 - Use externally authenticated batch users
 - Encrypt passwords in a file for automated jobs
 - Run automated jobs from the Oracle scheduler
 - Protect passwords in scheduling programs

Script: Reset Database Passwords

- **What:** When bringing a database into regulatory compliance, Oracle Profiles can be used to set expire times. Consider resetting the passwords before implementing profile changes
- **Why:** You don't want to expire all passwords at once.
- **How:** Reset passwords on a compliant database by:
 - Create a reset profile that does not contain password limitations.
 - Create a list of all users whose passwords require reset and the current profile setting for each user
 - Reassign each user's profile to the reset profile
 - Change each user's password to the current password
 - Reassign each user's profile to the correct security compliant profile
 - Drop the reset profile
- **See:** [ts_password_reset.sql](#)

Deploy Oracle Enterprise User Security

- **What:** Oracle Enterprise User Security can manage database users for multiple databases using a single LDAP repository in OID.
- **Why:** Users can change passwords routinely in one place, one time for policy compliance
- **How:** With an Oracle Internet Directory deployed:
 1. Tell the Database to use an LDAP directory
 2. Register the Database with OID
 3. Configure Enterprise Users:
 1. Match all users to a global database schema
 2. Match users to appropriate global database roles
- **Where:** See an Oracle How to at:
www.oracle.com/technology/deploy/security/db_security/howtos/eus-how-to.html

Link

Oracle Authentication to Active Directory

- **What:** Oracle authentication can be made with Microsoft Active Directory credentials
- **Why:** Users can have one password for the network and databases
- **How:** The major steps include:
 - configuration of an Oracle Internet Directory (OID) Server
 - configuration of a Microsoft Active Directory (AD)
 - modification of Oracle applications to use OID for authentication
 - synchronization of the OID and AD servers
- **Where:** See
 - Oracle Internet Directory Administrator's Guide 10g - Chapter 43 Integration with the Microsoft Windows Environment
 - Metalink note 267153.1 named "How To Setup OID Synchronization with Microsoft Active Directory Quick Start Guide".

Oracle Identity Management

- **What:** Oracle is beefing up in the Identity Management space with customer purchases and new products
- **Why:** Regulation and management is driving better authentication and provisioning
- **How:** Learn about Oracle offerings and deploy to your organization.

Configure the Oracle Listener Password

- **What:** The Oracle listener can require a password for administration
- **Why:** Prevent others from administering a password without authorization

- **How:**

```
LSNRCTL> set current_listener PREPLSNR
```

```
LSNRCTL> change_password
```

```
LSNRCTL> set password
```

```
LSNRCTL> save_config
```

- **Where:**

www.integrigy.com/info/Integrigy_OracleDB_Listener_Security.pdf

- **See:** [ts listener.txt](#)

Validate Listener Node Connections

- **What:** Use TCP.VALIDNODE_CHECKING to prevent and allow certain IP addresses from accessing database.
 - INVITED_NODES says which can connect
 - EXCLUDED_NODES says which can not
- **Why:** Restrict machines that can connect to known app-servers or DBA machines
- **Where:**
 - Oracle Security Step by Step by Finnigan – Step 5.2
 - Metalink note: 263030.1.

Validate Listener Node Connections (How)

```
edit sqlnet.ora...  
tcp.validnode_checking = yes  
# use either invited_nodes or excluded_nodes  
tcp.invited_nodes = (192.168.2.2,  
    192.168.2.3)  
# or...  
# tcp.excluded_nodes = (192.168.2.4)
```

Protect & Validate Backups

- **What:** Oracle Backups contain database contents and should be treated with care
 - **Why:** You don't want to be in the news
 - **How:** Avoid these mess-ups
 - Creating a backup of a database to disks where the backup disks are unprotected
 - Leaving tape backups in an unsecure location (desk, drawer, unlocked room and so on)
 - Disposing a tape backup without erasing the tape first.
 - Providing a tape backup to an unauthorized person
 - Exposing tapes to magnetic fields (mass transit)
- Instead – be sure to
- Define Clear roles and assignments
 - Use a bonded media retention vendor
 - Validate Backup with actual recovery
- **Where:** Note lost backups at www.privacyrights.org/ar/ChronDataBreaches.htm

Protect Backups with Encryption

- **What:** RMAN backups can be encrypted with key and Oracle Wallet (10r2)
- **Why:** Misplaced and stolen backups are protected by encryption
- **How:** Simple RMAN encryption-

```
RMAN> set encryption on;
```

```
RMAN> set encryption identified by 'cnetics';
```

```
RMAN> set encryption algorithm 'AES192';
```

```
RMAN> backup incremental level 0 database;
```

- **Where:** Oracle Database Backup and Recovery Advanced User's Guide at docs.oracle.com
- **See:** [ts rman encryption.txt](#)
- **Note:** Explore Oracle Secure Backup



Limit Privileges to Application Database User

- **What:** Many custom applications use a common database user to perform work on behalf of web clients. Strictly limit permissions for this user
- **Why:** A common user often provide a front door for web applications and application support people
- **How:** Check the system and object privileges for application user and revoke all but required

Separate Data Schema and Application Owners

- **What:** Code can be owned by a different database schema from the schema that owns the data on custom application.
- **Why:** A production support person can have powerful access to database tables
- **How:** In custom designs, separate the code owner by –
 - Placing database code in separate schema
 - Lock the database data schema
 - Provide access to application data tables by
 - Granting permissions via roles
 - Granting data access via stored packages

Wrap Stored Code

- **What:** Oracle reveals stored code in dictionary SOURCE views
- **Why:** Others can review algorithms, authentication and logic in stored database code
- **How:** Wrap then run the code

```
# host wrap iname=ts_secret_code.prc
SQL> @ts_secret_code.plb
```
- **Where:** PL/SQL User's Guide and Reference under the PL/SQL Wrap Utility.
- **See:** [ts_wrap.sql](#)

Hide Stored Code

- **What:** Users with ALL_SOURCE view and EXECUTE_ANY_PROCEDURE can see stored code
- **Why:** Others can review algorithms, authentication and logic in stored database code
- **How:** Revoke ALL_SOURCE from public and grant access through a role.

```
SQL> REVOKE SELECT ON ALL_SOURCE from PUBLIC;  
SQL> CREATE ROLE VIEW_CODE_ROLE;  
SQL> GRANT SELECT ON ALL_SOURCE to VIEW_CODE_ROLE;  
SQL> GRANT EXECUTE ANY PROCEDURE to VIEW_CODE_ROLE;
```

- **See:** [ts_all_source.sql](#)

Prevent SQL Injection Using Bind Variables

- **What:** Using bind variables forces checks on user input
- **Why:** SQL Injection attacks provide unauthorized access
- **How:** Without input checking and bind variables, browser input may be open to SQL Union query input. Place input into bind variables to execute in application.
- **Where:** See Tom Kyte “On Injecting and Comparing” in January 2005 Oracle Magazine
www.oracle.com/technology/oramag/oracle/05-jan/o15asktom.html

Use Roles for Privileges

- **What:** Object & system privileges can be grouped into roles.
- **Why:** Provide users the least privileges possible
- **How:** Create roles defined by business
 - Grant object permissions to roles
 - Grant system privileges to roles
 - Grant roles to users
 - Set default so role is not enable
 - Avoid using too many roles (performance & confusion)

Compliance by Documentation

- **What:** Auditors require documentation.
- **Why:** their job is too present evidence of compliance
- **How:** Generate documentation –
 - Use a technical writer
 - Find and note exceptions
 - Explain implementations of policies
 - Map regulation to implementation

Apply Oracle Patches

- **What:** Oracle provide quarterly patches
- **Why:** Regulators require patching and exploit code is available
- **How:** Find critical patches online and through email alert. Consider a schedule:
 - **Day 1:** The clock starts with notification of the Critical Patch Update.
 - **Day 2:** Identification of the patch
 - **Day 3:** Verification of the patch
 - **Day 4:** Installation of the patch on the Development Database
 - **Day 28:** Installation of the patch on the QA Database
 - **Day 60 (maintenance window):** Installation of the patch on Production Databases

Review Applied Patches

- **What:** Oracle provides OPATCH and Oracle Enterprise Manager Database control to note patch levels
- **Why:** Stay up to date on patch levels
- **How:** Use OPATCH & OEM

```
## opatch lsinventory
Oracle Interim Patch Installer version 1.0.0.0.53
Copyright (c) 2005 Oracle Corporation. All Rights Reserved.
Result:
Installed Patch List:
=====
1) Patch 4392423 applied on Tue Sep 13 12:11:29 EDT 2005
[ Base Bug(s): 4392430 4392423 4199455 4210374 ]
OPatch succeeded.
```

Manage CONNECT Role

- **What:** Oracle CONNECT role has many privileges prior to (10gR2)
- **Why:** Each user with CONNECT can create tables, database links and synonyms in their personal schema
- **How:** Create a different connect role or revoke privileges from Oracle's.

```
SQL> create role db_connect;
```

```
SQL> grant create session to db_connect;
```

```
SQL> grant db_connect to new_user identified  
by password;
```

- **See:** [ts connect role.sql](#)

Check Oracle File Permissions

- **What:** Oracle binary & configuration files have permissions that should be limited
- **Why:** Other users can tamper with key files
- **How:** Confirm ownership and permission of files and change if necessary
- **Where:** CIS benchmark for Oracle security at www.cisecurity.org/bench_oracle.html.
- **See:** [ts_os_files.sh](#)

Check Oracle File Permissions

```
# To check the ownership of the files in the $ORACLE_HOME,  
# list any that have owner != oracle OR group != oinstall:  
$$ (ORA_software_acct=oracle  
   ORA_dba_group=oinstall  
   find $ORACLE_HOME \  
   \\  
       \\  
       \(! -user $ORA_software_acct \) \  
   -o \\  
       \(! -group $ORA_dba_group \) \  
   \) \  
   -a -exec ls -ald {} \; \  
) 2>&1
```

```
# List "other" users with access to Oracle files  
$$ (find $ORACLE_HOME \  
   \\  
       \\  
       \(-perm -001 -o -perm -002 -o -perm -004 \) \  
   \) \  
   -a -exec ls -ald {} \; \  
) 2>&1
```

Disable Host Services

- **What:** Database servers do not require many host services
- **Why:** Limit the attack surface by disabling / removing unneeded services
- **How:** Depending on operating system, disable telnet, finger, sendmail, apache and so on.

Harden Database Parameters

- **What:** Certain Oracle database parameter settings yield stronger security.
- **Why:** Close more potential vulnerabilities
- **How:** Use the ALTER SYSTEM command or change the init.ora file
- **See:** [ts_spfile.sql](#)

Restrict Access Dictionary Views

- **What:** The Oracle dictionary provides information about database authentication, objects, code and permission.
- **Why:** Dictionary information is useful for exploit
- **How:** Limit access by
 - setting `O7_DICTIONARY_ACCESSIBILITY=FALSE`
 - limit `SELECT_CATALOG_ROLE` grants
 - Revoke public access to some views (`SYS.LINK$`)

SQL*Plus Product Security

- **What:** SQL*Plus capabilities can be limited via the PRODUCT_USER_PROFILE table
- **Why:** Control capabilities of users in SQL*Plus
- **How:** Create the product table

```
SQL> connect SYSTEM
```

```
SQL> @?/sqlplus/admin/pupbld.sql
```

– Insert rows into the table which control commands

- **Where:** SQL*Plus User's Guide and Reference at docs.oracle.com
- **See:** [ts_product_user_profile.sql](#)

Encrypt Data with Transparent Data Encryption

- **What:** Oracle 10gR2 provide easily configured database encryption with TDE
- **Why:** Regulations require some data be encrypted (PCI – Credit card numbers)
- **How:**
 - Configure Oracle Wallet
 - Encrypt column data with ALTER TABLE
- **Where:** Oracle Database Advanced Security Administrator's Guide 10g Release 2 (10.2) “Transparent Data Encryption” and Metalink Note: 317311.1
- **See:** [ts transparent data encryption.sql](#)

Encrypt Data with DBMS_CRYPTO

- **What:** Oracle supplies packages that encrypt and decrypt data
- **Why:** Regulations require some data be encrypted (PCI – Credit card numbers)
- **How:**
 - Choose encryption algorithm and key management policy/mechanism
 - Build code around `dbms_crypto` or `dbms_obfuscation_toolkit`
- **Where:** Encrypt your Data Assets at www.oracle.com/technology/oramag/oracle/05-jan/o15security.html
- **See:** [ts_dbms_crypto.sql](#)

Protect Export Data with Data Pump

- **What:** Oracle provides Datapump as an Export/Import Alternative and can re-encrypt database column data
- **Why:** Regulations require some data be encrypted (PCI – Credit card numbers)
- **How:**
 - Add an Encryption key to the export parameters
 - Use the Encryption key in the import parameters
- **Where:** Encrypt your Data Assets at www.oracle.com/technology/oramag/oracle/05-jan/o15security.html

Isolate Production Data

- **What:** Production data is often used for test and development systems
- **Why:** Regulations may require protection of all data.
- **How:**
 - Remove database links from test/development to production
 - Scramble sensitive production data on test systems
 - Generate new test/development data
 - Harden test/development like production

Data: Use Function & View to Mask Sensitive Data

- **What:** Sensitive data needs masking from most users
- **Why:** Regulations and policy require some information remain private
- **How:**
 - Create mechanism to authorize users (table, role, context)
 - Create a function to mask a value's contents
 - Revoke privilege on sensitive table from public
 - Create view that call function for the sensitive data column
 - Result: view provides unmasked data to authorized users
- **See:** [ts_masked_view.sql](#)

Use Virtual Private Database to Hide Data

- **What:** Virtual Private Database provides mechanism to hide rows & columns at the table level
- **Why:** Some table row & column data is sensitive and regulated.
- **How:**
 - Determine policy or function for column display
 - Use DBMS_RLS to attach policy to sensitive table
- **Where:** “Virtual Private Database” in the Oracle Database Security Guide at docs.oracle.com
- **See:** [ts vpd rows.sql](#) & [ts vpd columns.sql](#)

Explore Database Vault

- **What:** New Oracle feature called Database Vault to be released
- **Why:** Protect sensitive data, even from SYSDBA access
- **How:** Administrator can specify “Realms” within the database to protect all access.

Secure your Website against “Filetype” searches

- **What:** Files may exist on your website that are not linked yet may be found by search engines
- **Why:** Staff may believe these files are safe because they are hidden
- **How:** Search on a website by filetype

`filetype:xls www.cnetics.com`

- **Where:** See Google help about file type searches at www.google.com/help/features.html

60 Security Tips

60
MINUTES

Save the Date!



COLLABORATE07
Technology and Applications Forum for the Oracle Community

April 15 - 19, 2007
Mandalay Bay Resort and Casino
Las Vegas, Nevada

Cnetics
www.cnetics.com

Submit to present for the IOUG!

Share your expertise with the greater Oracle community. Solidify your reputation as an Oracle expert! The IOUG is looking for presentations in the following tracks:

Architecture, Database, Development, and
Middleware.

Cnetics

Submit your abstracts no later than

Use Standard Oracle Auditing Efficiently

- **What:** Configure Oracle standard auditing to capture useful information
- **Why:** Avoid filling audit systems with useless information
- **How:** Set up database with information about
 - Changes to the audit trail table
 - Changes in audit settings
 - Escalation of privileges
 - Provisioning
 - Schema changes
- **See:** [ts_audit_setup.sql](#)



Audit User Logins and Report Results

- **What:** Oracle provides connection auditing to capture connections.
- **Why:** Protect database access and capture connections for forensics in the event of a breach.
- **How:** Turn on auditing of sessions and query DBA_AUDIT_SESSION
- **Where:** Pete Finnigan "Introduction to Simple Oracle Auditing"
www.securityfocus.com/infocus/1689
- **See:** [ts_audit_sessions.sql](#)

Audit User Logins and Report Results (...)

```
set newpage 2
set heading off

select count(*) Num,
       substr(username,1,10) username,
       substr(terminal,1,12) terminal,
       substr(os_username,1,15) os_username,
       substr(to_char(timestamp, 'DD-MON-YY'), 1, 9)
timestamp
from dba_audit_session
where returncode<>0
and timestamp > sysdate-7
group by username,
       terminal,
       os_username,
       to_char(timestamp, 'DD-MON-YY');
```



Use Extended Auditing in 10g

- **What:** Oracle Extended Auditing provides SQL & bind values to the audit trail
- **Why:** SQL & bind values improve breach forensics
- **How:** Change the AUDIT_TRAIL parameter
- **Where:** Find more information in [Chapter 11](#) of the *Oracle Database Security Guide 10g Release 1 (10.1)*.

Audit - Use Oracle 10g's Extended Auditing (...)

```
ALTER SYSTEM SET AUDIT_TRAIL = DB_EXTENDED SCOPE=SPFILE;  
audit insert, update, delete on scott.emp by access;  
Startup force;
```

```
-- Update the SCOTT.EMP table with a bind variable  
execute :salary := 7000;  
update SCOTT.EMP set sal = :salary where empno = 9000;
```

```
-- Query the audit trail and see SQL and bind variables  
select owner, obj_name, action_name, sql_bind, sql_text  
       from dba_audit_trail;
```

One Oracle returned for the update statement shows the SQLTEXT and the SQLBIND values like this:

```
SQLTEXT -> update SCOTT.EMP set sal = :salary  
           where empno = 9000
```

```
SQLBIND -> #1(4):7000
```



Audit SYS Database Activity

- **What:** Oracle Standard auditing does not capture actions by users connected as SYSDBA to the audit trail. Trace files can be written for SYSDBA activities with a DB parameter setting
- **Why:** Regulations require all “root” level access audited
- **How:** Set the database parameter –
`alter system set audit_sys_operations=TRUE scope=spfile;`
- **See:** [ts_audit_sys_user.sql](#) & [audit_sys_user.sh](#)

Monitor the Status of Auditing

- **What:** Oracle Standard auditing, dictionary views can be viewed to confirm audit settings.
- **Why:** Watch for unexpected changes to audit options active in the database
- **How:** Review the contents and changes to three data dictionary views:
DBA_PRIV_AUDIT_OPTS,
DBA_STMT_AUDIT_OPTS and
DBA_OBJ_AUDIT_OPTS.
- **See:** [audit monitor status.sql](#) and [monitor audit status.sh](#)

Manage the Audit Trail

- **What:** Oracle provides mechanisms for tracking changes to the audit trail
- **Why:** Regulations require changes to audit trail to be tracked
- **How:** For database auditing:
 - ❑ Set up auditing of changes to auditing
 - ❑ Audit access to the SYS.AUD\$ table
- **See:** [ts_audit_auditing.sql](#)

```
-- audit the audit and no audit statements
audit system audit;
-- audit changes made to the audit trail
audit select, insert, update, delete on sys.aud$ by access;
```

Manage the Audit Trail

- **What:** Audit information written to the Oracle audit trails either in database or on OS can be copied to an offline server
- **Why:** The audit trail must be preserved and protected from DBA tampering
- **How:** Create automated job to routinely write DB or OS audit trail to a remote machine by:
 - Copying the files with secure copy
 - Emailing the files to a secure email address
 - Include other audit trails like Fine grained auditing (DBA_FGA_AUDIT_TRAIL)

Create an XML Audit Trail

- **What:** The Oracle OS Audit trail can be XML (10gR2)
- **Why:** The OS Oracle audit trail is difficult to decipher
- **How:** Change the audit_trail database parameter

```
alter system set audit_trail = OS scope = spfile;  
Startup force;  
AUDIT UPDATE ON SCOTT.EMP;  
update SCOTT.emp set sal = 10000;
```

```
Audit trail: SESSIONID: "859" ENTRYID: "2" STATEMENT:  
↳ "7" USERID: "SCOTT" USERHOST: "KENNY-DESK"  
↳ TERMINAL: "KENNY-DESK" ACTION: "103" RETURNCODE:  
↳ "0" OBJ$CREATOR: "SCOTT" OBJ$NAME: "EMP" SES$ACTIONS:  
↳ "-----S-----" SES$TID: "52556" OS$USERID:  
↳ "ksmith"
```

Create an XML Audit Trail (...)

```
alter system set audit_trail = XML scope = spfile;
Startup force;
update SCOTT.emp set sal = 10000;
```

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Audit xmlns="http://xmlns.oracle.com/oracleas/schema/dbserver_audittrail-10_2.xsd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.oracle.com/oracleas/schema/dbserver_audittrail-10_2.xsd">
  <Version>10.2</Version>
  - <AuditRecord>
    <Audit_Type>1</Audit_Type>
    <Session_Id>868</Session_Id>
    <StatementId>1</StatementId>
    <EntryId>1</EntryId>
    <Extended_Timestamp>2006-04-02T16:38:35.781000</Extended_Timestamp>
    <DB_User>SCOTT</DB_User>
    <OS_User>CNETICS\ksmith</OS_User>
    <Userhost>CNETICS\KENNY-DESK</Userhost>
    <OS_Process>904:660</OS_Process>
    <Terminal>KENNY-DESK</Terminal>
    <Instance_Number>0</Instance_Number>
    <Action>100</Action>
    <Returncode>0</Returncode>
    <Comment_Text>Authenticated by: DATABASE</Comment_Text>
  </AuditRecord>
  + <AuditRecord>
  + <AuditRecord>
</Audit>
```

Track Activity on Host Machine with Sudo

- **What:** Unix system activity can be tracked with sudo
- **Why:** Regulation and forensics require information of administrative host system accounts
- **How:** Install sudo and lock root and oracle access, forcing users to login as themselves
- **Where:** www.courtesan.com/sudo/
- **See:** [ts sudo.txt](#)

Audit Access to Sensitive Tables (FGA)

- **What:** Oracle provides Fine Grained auditing for capturing access to sensitive tables
- **Why:** Regulation require a trail of user access to sensitive table information
- **How:** Implement policies to capture queries to a database audit trail using the supplied dbms_fga package.
- **Where:** Arup Nanda article on FGA at www.oracle.com/technology/oramag/webcolumns/2003/techarticles/nanda_fga.html

Filter Fine Grained Auditing

- **What:** FGA can audit a specific columns on a table with specific conditions
- **Why:** Capture only meaningful data access events
- **How:** Create a function to determine if the query event matters. Then set up that function as part of the AUDIT_CONDITION for FGA

```
AUDIT_CONDITION = (is_salary_ok(username) = 'YES')
```

View Common Audit Data in DBA_COMMON_AUDIT_TRAIL

- **What:** Both standard Oracle Auditing and FGA auditing data can be viewed from a single view
- **Why:** Forensics can be captured for all Oracle activity except SYSDBA
- **How:** after setting up Oracle standard and FGA auditing, query the DBA_COMMON_AUDIT_TRAIL for combined audit information
- **Where:** see Oracle Reference for information on this view.

Audit Database with LogMiner & Streams

- **What:** Oracle redo reveals database activity valuable to auditing data changes. Use Logminer & Streams
- **Why:** Data in the redo stream cannot be changed by the DBA
- **How:** Set up Logminer by:
 - Capturing supplemental redo information
 - Start Logminer with `dbms_logmnr`
 - View contents in `V$LOGMNR_CONTENTS`
 - Stop Logminer with `dbms_logmnr`
- **See:** [ts redo.sql](#) & the Oracle Streams Concepts and Administration 10g manual

Audit Using Client Context

- **What:** User contexts can be captured in the audit trail
- **Why:** Additional client information is valuable in forensics
- **How:** Configure applications to set contexts that is captured to the audit trail.

```
DBMS_SESSION.SET_CONTEXT ('APP_CTX', 'APP_USERID',  
    p_user_id);  
DBMS_SESSION.SET_IDENTIFIER (p_user_id);  
SELECT DB_USER, CLIENT_ID FROM DBA_FGA_AUDIT_TRAIL;
```

- **Where:** See Nanda's article on FGA (part 2)
www.oracle.com/technology/pub/articles/nanda_fga_pt2.html

Configure Flashback for Forensics

- **What:** Oracle Flashback allows you to see historical (previous) data values
- **Why:** When investigating a breach, data changes over a time interval may be helpful
- **How:** Configure Flashback on the database and query data and dictionary views to use & manage flashback
- **Where:** Review Oracle Documentation on flashback – Flashback Database - download-east.oracle.com/docs/cd/B19306_01/server.102/b14200/statements_9011.htm#SQLRF01801
- **See:** [ts flashback.sql](#)

Audit Vault is Coming

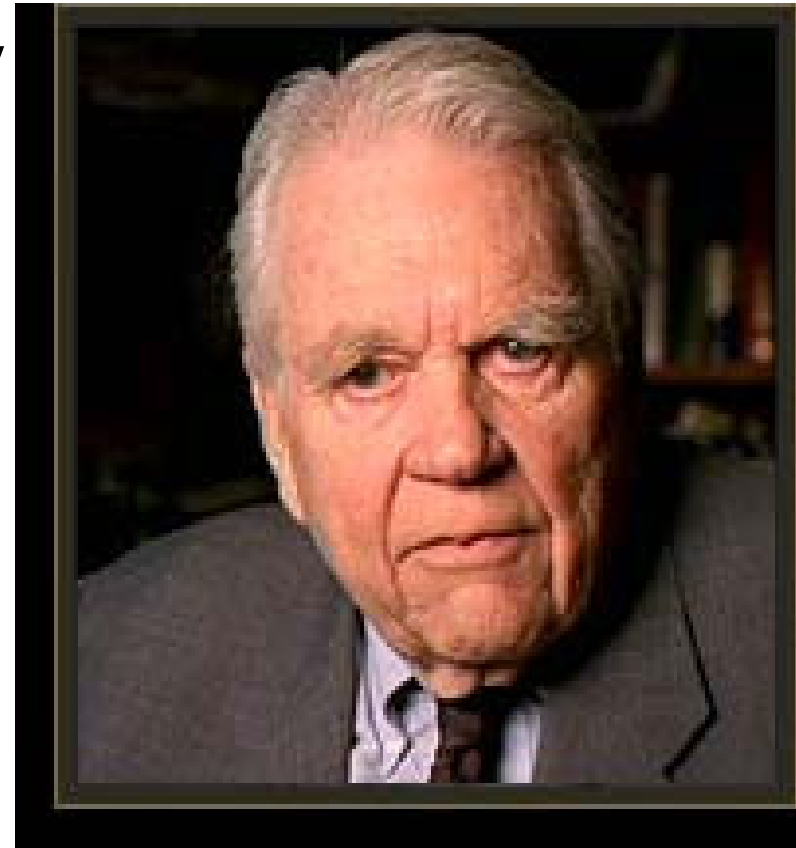
- **What:** Oracle is developing a new feature named Audit Vault for storing and mining audit trails from multiple databases
- **Why:** Reviewing and managing current audit trails is cumbersome
- **Where:** See Paul Needham's IOUG presentation and online at [ORACLE AUDIT DIRECTIONS FOR PRIVACY & COMPLIANCE](#)

Follow the Oracle Security Checklist

- **What:** Free checklists are available to help you remember security items to check
- **Why:** Provides assistance for securing your database
- **How:** Review lists in products and online
- **Where:** See these check lists:
 - Oracle Database Security Checklist at www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
 - CI Security Oracle Benchmark – www.cisecurity.org
 - SANS Checklist by Pete Finnigan - www.petefinnigan.com/orasec.htm

And Now – Andy Rooney

- Have ever wondered why database people feel like they have to do everything alone and by themselves?
- Join the IOUG Oracle Security Special Interest Group (SIG) “Enterprise Best Practices”



60 Security Tips

60
MINUTES

60 Oracle Security Tips in 60 Minutes

For Scripts email –
kenny.smith@cnetics.com

Cnetics
www.cnetics.com