



# OracleX Oracle 10g and Beyond

Presented by Aaron Grothe  
ajgrothe@yahoo.com


CISSP, Security+, Oracle 10g DBA

NebraskaCERT Conference 2004






# Intro

- ⇒ With their latest release of the Oracle 10g database Oracle has made the life of DBAs and CSOs much easier
  - ⇒ We'll go over some of the changes and some general Oracle Database Security tips that help balance between a “perfectly” secure database and a usable one
- 




# Overview

- ⇒ Speaker Intro
  - ⇒ Oracle Security Alerts
  - ⇒ Unbreakable my Fanny
  - ⇒ Oracle 10g Database Improvements
  - ⇒ Oracle Auditing
  - ⇒ Misc Tools
  - ⇒ Resources
  - ⇒ Q & A
- 




# Speaker Intro

- ⇒ “Who am I? Why am I here?” - Admiral Stockdale at Vice Presidential Debate 1992
  - ⇒ My background – I was a DBA at infoUSA a large corporation that lives/dies by the database
  - ⇒ I have taken the Oracle 10g database assessment exam so I do have the ability to use the “Oracle 10g DBA” - Given out by Oracle University
- 



# Speaker Intro

- ⇒ I am not always right :-)
  - ⇒ “I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386 (486) AT clones.” - Linus Torvalds 1991
  - ⇒ I thought this will be another flash in the pan
  - ⇒ I was **WRONG**
  - ⇒ If I'm going to fast **SPEAK UP!!!**
  - ⇒ If you have a question, please let me know
- 



# Oracle Security Alerts

- ⇒ How many are signed up for Oracle Security Alerts?
  - ⇒ URL to sign up for Alerts
    - ⇒ <http://www.oracle.com/technology/deploy/security/>
    - ⇒ User needs a free OTN-account
    - ⇒ To get most patches need a metalink account which requires current support contract
  - ⇒ Lets Look at an example Alert
- 




# Oracle Security Alerts

- ⇒ CERT <http://www.cert.org> is another good resource
  - ⇒ Currently no exploits for Oracle 10g DB
- 




# Oracle Security Alerts

- ⇒ Also need to be signed up for the security alerts of the underlying Operating System
  - ⇒ E.g. Red Hat <http://www.redhat.com/security>
  - ⇒ A lot of issues can be reduced by turning on the local system's firewalling capabilities  
E.g. Linux-iptables/netfiler, Sun's Firewall  
Sunscreen has a reduced capability system shipped with O/S
- 






# Oracle Security Alerts

- ⇒ Creating a consistent patching/deployment policy is important for everybody
    - ⇒ Sarbanes-Oxley pushes new rules about Data Privacy
    - ⇒ HIPPA raises some potential issues
    - ⇒ Loss of revenue, trust and goodwill caused by a disclosure can be almost impossible to measure or recover from
- 



# Unbreakable My Fanny

- ⇒ Shortly after Oracle announced their Database was “unbreakable” in 2002 David Litchfield found several buffer overflow vulnerabilities in Oracle 9i
  - ⇒ Some of the problems were present in Oracle 8 in 1988
  - ⇒ Oracle has changed the Unbreakable marketing campaign to being more about availability versus being Secure
- 




# 10g Database Improvements

- ⇒ Reduced Install Size
  - ⇒ Patching Design
  - ⇒ Default Accounts
  - ⇒ New OEM Oracle Enterprise Manager
- 



# Reduced Default Install Size

- ⇒ With 10g Oracle has reduced the install size from 3 cds to 1 cd and the corresponding disk space from 5gb to 2gb (usually)
    - ⇒ This reduces the amount of optional components that are usually installed
    - ⇒ A lot of security alerts have to do with Product A with Option X installed, this reduces the number of avenue of attacks
- 




# Patching Design

- ⇒ Anatomy of installing a patch on an Oracle 8i system to provide a methodology to back the patch out
  - ⇒ Backup the whole system (O/S level and database level)
  - ⇒ Install tripwire or similar package and run to get good checksums
  - ⇒ Install new patch
  - ⇒ Run tripwire again to get delta between two systems






# Patching Design (Cont)

- ⇒ Offer animal sacrifice to the Oracle Gods
  - ⇒ Test see if patch resolves issue
  - ⇒ If not. Determine whether to attempt to back patch out of system or simply restore whole system from backups
  - ⇒ Make sure to keep track of patch number that has been installed there is no guaranteed way to tell what patches have been installed
  - ⇒ Repeat for next machine
- 



# Patching Design (Cont)

- ⇒ There are other ways to deal with this issue one of which is a package called Ringmaster.  
Ringmaster is a commercial product that is rather expensive, but in a commercial environment can be worth EVERY penny
  - ⇒ Some people have offered patches converted to the same format as the underlying Operating System E.g. RPMs for Redhat machines, but these aren't official patches
- 



# Patching Design (Cont)

- ⇒ Oracle 10g Oracle Enterprise Manager (OEM) offers the ability to download and install patch, you can even schedule when to install patch
  - ⇒ It even provides the ability to back patch out
  - ⇒ Can even allow deployment to multiple machines
  - ⇒ Also can show the user new patches when they become available
- 






# Patching Design (Cont)

- ⇒ Sounds pretty basic, but this one change alters the whole world for a lot of DBAs






# Default Accounts

- ⇒ Oracle 8 and 9 by default create several accounts when a new database is created.
  - ⇒ E,g, Default password for Sys account is “change\_on\_install”
  - ⇒ In my experience at least 10% of databases I've looked at have at least one account with default password enabled
  - ⇒ This is easily scriptable and a lot of tools exist to do just this
- 




# Default Accounts

- ➔ Oracle 10g changes that, when a database is created it locks the majority of accounts and asks the user to set a password for the most important accounts `sys/sysdba` and the like
  - ➔ Scott/Tiger is a thing of the past
- 



# New OEM

- Oracle has totally reworked the Oracle Enterprise Manager for 10g. It is now much closer to the design of the Oracle 9ias control panel.
  - It is available through the web, allowing monitoring on systems without the client software installed
- 




## New OEM (cont)

- ⇒ OEM 10g provides information about usage of the system which can be an indicator of abuse of the system.




# Things not discussed

- ⇒ Virtual Private Databases
  - ⇒ Fine Grained Auditing
  - ⇒ Data encryption DBMS\_CRYPTO
  
  - ⇒ The following is a good resource for examples of the above  
<http://www.oracle-base.com/articles/10g/Databa>
- 




# Oracle 10g Summary

- ⇒ RUN!!! Don't walk to Oracle 10g it is the single most important upgrade to Oracle since at least 8i
  - ⇒ Caveat Oracle 10g is still young. A lot of production systems are still running on older versions and have no plans of updating for some time
- 




# Oracle 10g Summary

- ⇒ Oracle 10g does not at the time of this talk support running Oracle Financials, so you can't upgrade that component yet. Oracle is hard at work on this though.
  - ⇒ Oracle 10g also forces changes to certain 9i features such as the CBO instead of the RBO and the like which can cause quite a bit of pain and suffering
- 






# Oracle Auditing

- ⇒ Creating an effective auditing policy is vital to keeping the data in your database safe
  - ⇒ Oracle provides a huge variety of auditing options. We'll cover just a few to create a simple/easy audit policy for a system
  - ⇒ The audit procedures should work on Oracle 8i/9i/10g systems with minimal changes
- 




# Oracle Auditing

- ⇒ Why Audit?
  - ⇒ Why Not Audit?
  - ⇒ How to Audit
  - ⇒ How Not to Audit
  - ⇒ Basics
- 




# Why Audit

- ⇒ We already have a firewall/ids/os audit package/single sign on/magic beans
  - ⇒ Most company networks aren't well segmented
  - ⇒ Audit trail can help with troubleshooting database issues
  - ⇒ An audit trail can be valuable to reconstruct a database
- 



# Why Not Audit

- ⇒ Audits can slow system – typical auditing should result in a 5% database impact – if you audit more the impact will be higher
  - ⇒ Poorly implemented audit policy can lead to a false sense of security
  - ⇒ A badly implemented audit policy can result in the inability to convince management to accept an audit policy in the future
- 



# How to Audit

- ⇒ Incremental
  - ⇒ Build on Goals
  - ⇒ Regularly “truncate” audit trails do no delete
  - ⇒ Work with Security Office
  - ⇒ Size tables appropriately
- 




# How NOT to Audit

- ⇒ All or nothing
- ⇒ Regularly “delete” audit table entries or better yet never get rid of entries






# O/S Auditing or DB Auditing

- ⇒ If you are using syslog-ng and already have an audit policy defined, using system logging might be a good fit
  - ⇒ Aggregation of multiple database results is possible with O/S level auditing
  - ⇒ Different Operating systems provide different levels of auditing functionality
  - ⇒ Does DBA have access to O/S audit trail?
- 




# Examples

- ➔ Based on Pete Finnigan's work and the O'Reilly Oracle Security book
  - ➔ Showing connection attempts
  - ➔ Failed log-on attempts
  - ➔ Failed log-on attempts with return codes
  - ➔ Attempts to access the database with non-existent users
  - ➔ Access attempts at unusual hours
  - ➔ Users accessing database accounts from multiple locations
- 






# Examples

- ⇒ Multiple user accessing database from same location
  - ⇒ Objects being created or changed
- 




# Showing connection attempts

- ⇒ Select username, terminal, action\_name, to\_char(timestamp, 'DDMMYYYY:HHMISS') timestamp, to\_char(logoff\_time, 'DDMMYYYY:HHMISS') logoff\_time, returncode \* from dba\_audit\_session
  - ⇒ Output
    - ⇒ Username Timestamp Terminal Logoff\_time Action Returncode
- 




# Showing connection attempts

- ⇒ Select count(\*), username, terminal, to\_char(timestamp, 'DDMMYYYY:HHMISS') from dba\_audit\_session where returncode <> 0 group by username, terminal, to\_char(timestamp, ('DD-MON-YYYY');
  - ⇒ Output
    - ⇒ Number of failed attempts, username, terminal timestamp
- 




# Showing connection attempts

- ⇒ Select count(\*), username, terminal, to\_char(timestamp, 'DDMMYYYY:HHMISS') from dba\_audit\_session where returncode <> 0 group by username, terminal, to\_char(timestamp, ('DD-MON-YYYY'));
  - ⇒ Output
    - ⇒ Number of failed attempts, username, terminal timestamp
- 



# connection attempts with invalid users


- ⇒ Select username, terminal, to\_char (timestamp, 'DDMMYYYY:HHMISS') from dba\_audit\_session where returncode <> 0 and not exists (select 'x' from dba\_users where dba\_users.username=dba\_audit\_session.username)
  - ⇒ Output
    - ⇒ Invalid usernames, timestamps, terminal
- 

# Access at Unusual Hours

- ➔ Select username, terminal, action\_name, returncode, to\_char(timestamp, 'DD-MON-YYYYHH24:MI:SS') to char(logoff\_time, 'DD-MON-YYYYHH24:MI:SS') from dba\_audit\_session where to\_date(to\_char(timestamp, 'HH24:MI:SS'), 'HH24:MI:SS') < to\_date('08:00:00', 'HH24:MM:SS') or to\_date(to\_char(timestamp('HH24:MI:SS'), 'HH24:MI:SS')) < to\_date('19:30:00', 'HH24:MI:SS')




# Access at Unusual Hours

- ⇒ Output
    - ⇒ Username
    - ⇒ Terminal
    - ⇒ Action
    - ⇒ Returncode
    - ⇒ Timestamp
- 




# Users accessing Database Multiple Locations

- ⇒ Select count(distinct(terminal)), username from dba\_audit\_session having count (distinct(terminal))>1) group by username
  - ⇒ Output
    - ⇒ Username
    - ⇒ Number of Terminals user connected from
- 






# Multiple Users One Location

- ⇒ Select `count(distinct(username))`, terminal from `dba_audit_session` having `count(distinct(username))>1` group by terminal
  - ⇒ Output
    - ⇒ Terminal
    - ⇒ Number of accounts logged in from this location
- 





# Objects being Created/Changed

- ⇒ Select username, priv\_used, obj\_name, to\_char (timestamp('DD-MON-YYYY HH24:MI') timestamp returncode from dba\_audit\_session where priv\_used is not null and priv\_used <> 'CREATE SESSION'
  - ⇒ Output
    - ⇒ Username, Privelege used
    - ⇒ Object accessed, Time, Return Code
- 



# What does this do for us?

- ⇒ Potential abuse of the database
  - ⇒ Shared accounts
  - ⇒ Modification of objects
- 
- 




# Other potential auditable events

- ⇒ Audit changed/original values for important tables
  - ⇒ Payroll/Vacation time
- ⇒ Audit attempts to view database
- ⇒ Summarize results into another table to preserve results and truncate database table






# Performance Suggestsions

- ⇒ Do not index audit tables
  - ⇒ Put on separate disks or less used drives
  - ⇒ Put audit trail in own table space
  - ⇒ Turn off triggers when doing bulk operations  
massive adds/deletes
- 




# Misc

- ⇒ What happens when tablespace is full
    - ⇒ Trusted Oracle stops processing
    - ⇒ Regular Oracle will keep going, triggers will fail since attempt to audit will fail
  - ⇒ Rollbacks will also rollback the audit trail preventing the existence of non-existent audits
    - ⇒ PRO/CON???
- 



# Example Implementation

- ⇒ At my former employer there was a huge push for database auditing
    - ⇒ Given the failed experiment years ago, there was tremendous pushback on the auditing plans
    - ⇒ Never got off test database machines
    - ⇒ Sarbanes-Oxley is supposed to be reviving project
- 



# Summary Auditing


- ⇒ Oracle's auditing facilities are amazing
  - ⇒ Enough rope to hang yourself and all your coworkers
  - ⇒ Used with caution and incremental change can be a very powerful tool








# Resources (10g Improvements)

- ➔ Oracle's Home page <http://www.oracle.com>
  - ➔ Unbreakable Oracle by Design: Oracle Database 10g Security by David Knox
  - ➔ Security Focus Pete Finnigan's Series on Oracle Security
  - ➔ Oracle Database Checklist  
[http://www.sans.org/score/checklists/Oracle\\_](http://www.sans.org/score/checklists/Oracle_)
- 




# Resources (Audits)

- Oracle's Home page <http://www.oracle.com>
  - Oracle's technet page [otn.oracle.com](http://otn.oracle.com)
  - Oracle Security Handbook by Marlene Theriault and William Henry O'Reilly Press 1998 ISBN 1-56592-450-9
  - Oracle Security step-by-step A survival guid for Oracle Security Pete Finnigan 2003, published by SANS institute
  - Finnigan's Home Page <http://www.petefinnigan.org/orasec.html>
- 




# Resources (Audits)

- Oracle's Home page <http://www.oracle.com>
  - Oracle's technet page [otn.oracle.com](http://otn.oracle.com)
  - Oracle Security Handbook by Marlene Theriault and William Henry O'Reilly Press 1998 ISBN 1-56592-450-9
  - Oracle Security step-by-step A survival guid for Oracle Security Pete Finnigan 2003, published by SANS institute
  - Finnigan's Home Page <http://www.petefinnigan.org/orasec.html>
- 



# Misc Tools

- ⇒ Oracletool – Great high level tool  
<http://www.oracletool.com/download.html>
  - ⇒ Karma – Big Brother for Databases  
<http://www.iheavy.com/karma/>
  - ⇒ Book Oracle & Open Source  
<http://www.oreilly.com/catalog/oracleopen/>
- 



# Q & A

⇒ Questions???

⇒ Thank You

