Secure Your Database in a Single Day

Arup Nanda
Starwood Hotels

© Arup Nanda, 2007
Who I Am

• An Oracle DBA for 14 years
• Lead DBA at Starwood Hotels
• Written some papers, speaks at conferences, three books
• Services – Security Audits, Security Preparedness, Backup Planning, RAC Setup, etc.
Why This Session

- Security is an often misunderstood area with a lot of “myths”
- Some examples:
  - Encryption is absolutely necessary
  - You should not use port 1521 for listener
  - Listener name should not be “LISTENER”
  - Database server must be behind a firewall
  - If you have a firewall, you don’t need to worry
  - Any decent security implementation takes a long time and lot of effort (and money)
Security Must be Layered

External Firewall

Internal Firewall

Authentication

Authorization
Plan of Attack

- Quick Compliance
- Long Term
- Low Hanging Fruit
- Nice to Have

Easier to Difficult

High Impact

Implementation
What You’ll Learn

• What you can do, in a single day
• 30 Carefully planned actions
• Addresses three Areas:
  – Identify and Seal Vulnerabilities
    • OS
    • Database
  – Build a Monitoring System
  – Enforce Change Control
• It will accomplish 60% of the compliance
• Each recommendation has – pros, cons and impact
• Take away scripts (please see the scripts.txt file or download from www.proligence.com)
Prelims

• Physical Security
  – Access control to the server
  – Authentication (unix userid password, etc.)
  – Surveillance and Auditing
  – OS Level Security – patches, unknown users, etc.

• Oracle specific
  – OS Vulnerabilities, including Listener
  – Database Vulnerabilities
Protecting the Oracle Account

- Institute an indirect login policy
- All users directly logging in can be mapped to real persons
  - su - oracle
- This leaves an audit trail of account logins
Listener Information

- Information from Listener
  SERVICES
  RAWMODE

- Remote Listener
  - Place an entry in LISTENER.ORA
  LSNRCTL> set current_listener ip_address
  LSNRCTL> set RAWMODE on
  LSNRCTL> services
Listener Denial of Service

• Stopping the Listener Maliciously
  – LSNRCTL> stop
  – LSNRCTL> set startup_waittime 20
    • This will prevent from accepting connections up to 20 seconds, enough time for the adversary to stop it.
• An attacker can loop through this logic to stop the listener forever.
Listener as a Launchpad

- Vandalism in redo log files
  - LSNRCTL> set log_file dumb
  - This command creates a file named dumb.log
  - LSNRCTL> set log_directory ‘/tmp’

- Hacker can use it to replace online redo log files by specifying the redo log directory and name.

- Best Practice: Do not use “log” as extension for Online Redo Logs; use “redo”, e.g. redo1.redo
Prevention

• Disable Online Modification
  – `ADMIN_N_RESTRICTIONS_<ListenerName> = ON`
  – This will force values to be changed in `LISTENER.ORA` and then listener reloaded.

• Set a password
  `LSNRCTL> change_password`
  `LSNRCTL> save_config`
Oracle 10g Issues

• Listener Protection is in 2 ways:
  – OS Authentication
  – Password
• Disable OS Authentication
  – Undocumented parameter in listener.ora
  – \texttt{LOCAL\_OS\_AUTHENTICATION\_<ListenerName> = OFF}
Ramifications

• Password required for all key listener operations but not to startup
• Enterprise Manager Grid Control will fail to identify the Listener. Solution: create the listener using GC.
• Oracle Real Application Cluster (RAC) CRS does not know the password. So it will report the listener as offline.
Permissions Issues

• The “oracle” executable

$ ls -l oracle
-rwsr-s--x 1 oracle oinstall 69344968 Jun 10 14:05 oracle

```
Type  Owner  Group  Others
-  r   w   s  r   -  s  -   -   x
```

**ananda:** sqlplus scott/tiger

© Arup Nanda, 2007
Two Task Architecture

- sqlplus
  - Running under ANANDA

- Server process
  - Running under ORACLE

Database

© Arup Nanda, 2007
Server Process

$ sqlplus scott/tiger
$ ps -aef | grep sqlplus
  ananda  6339  6185  0 13:06 pts/0  00:00:00
  sqlplus
$ ps -aef | grep 6339
  ananda  6339  6185  0 13:06 pts/0  00:00:00
  sqlplus
  oracle   6340  6339  0 13:06 ?      00:00:00
  oraclePRODB1
      (DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=beq)))

Client Process

Server Process

© Arup Nanda, 2007
Change Permission

• Remove SUID
  
  ```
  $ chmod 0700 $ORACLE_HOME/bin/oracle
  ```

• New Permissions
  
  ```
  -rwx------ 1 oracle oinstall 248754168 Oct 8 07:11 oracle
  ```

• Test
  
  ```
  $ sqlplus scott/tiger
  ```
  
  The user will immediately get an error.

  ```
  ERROR:
  ORA- 12546: TNS: permission denied
  ```
Fix

• Add in TNSNAMES.ORA

  PRODB2 =

  (DESCRIPTION =
   (ADDRESS_LIST =
     (ADDRESS = (PROTOCOL = TCP)
      (HOST = prolin2)(PORT = 1521))
   )
  )

  (CONNECT_DATA = (SERVICE_NAME = PRODB2))

• $ sqlplus scott/tiger@prodb2

• Install a new Oracle Home for the clients and let them use the SQLPLUS there. This OH is owned by apps group.
Other Executables

• Find them:

```bash
find . -type f \(( -perm -2000 -o -perm -4000 \) -exec ls -l {} \;

– oracle0. chown 0000
– oradism
– emtgtctl2 – EM Agent. chown 0700
– nmb – Grid Control Agent
– nmo - Grid Control Agent
– extjob and extjob0 – 0700
```
Other Executables

- **DBSNMP**
  - `rwsr-s---` 1 root dba 2986836 Jan 26  2005 dbsnmp
  - Change it.
    - `chown oracle:dba dbsnmp`
    - `chmod 0700 dbsnmp`

- lsnrctl and (lsnrctl0) and tnslsnr (and tnslsnr0)
  - `ls -l *lsnr*`
    - `-rwxr-x--x 1 oracle oinstall 214720 Oct 25 01:23 lsnrctl`
    - `-rwxr-x--x 1 oracle oinstall 1118816 Oct 25 01:23 tnslsnr`
  - Change them
    - `$ chmod 700 lsnrctl tnslsnr`
    - `$ chmod 000 lsnrctl0 tnslsnr0`
Configuration File Perms

- No Oracle Configuration file should have any privilege to others
  
  `-rwxr-xr-x 1 orandsp oinstall 779 Jun 16 03:59 listener.ora`
  
- No need to have read and execute permissions to `listener.ora`. Password can be made visible.

- Change permissions of `listener.ora`, `init.ora`

- Do not change: `sqlnet.ora` and `tnsnames.ora`
External Procedure

• Entry in listener.ora
  
  \[
  \text{(ADDRESS\_LIST} = \text{(ADDRESS} = \text{(PROTOCOL} = IPC) \\
  \text{(KEY} = \text{EXTPROC}))
  \]

• The user executes a program \textit{as the user oracle}!
  – Can delete data files, steals data, and so on

• Solutions:
  – Remove the lines
  – Move it to a different listener
  – Separate it to different listener.ora file
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = TCP)(HOST = ANANDA)(PORT = 1521))
      )
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = IPC)(KEY=ANANDA))
      )
    )
  )
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = ANANDA)
      (ORACLE_HOME = d:\ora9)
      (SID_NAME = ANANDA)
    )
    (SID_DESC =
      (GLOBAL_DBNAME = ANANDA)
      (ORACLE_HOME = d:\ora9)
      (SID_NAME = ANANDA)
    )
  )
SID_LIST_LISTENER_EXTPROC =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = ANANDA)
      (ORACLE_HOME = d:\ora9)
      (SID_NAME = PLSExtProc)
      (PROGRAM = extproc)
    )
    (SID_DESC =
      (GLOBAL_DBNAME = ANANDA)
      (ORACLE_HOME = d:\ora9)
      (SID_NAME = ANANDA)
      (PROGRAM = extproc)
    )
  )

© Arup Nanda, 2007
Hiding Passwords

- `sqlplus scott/tiger @myscript`
- `sqlplus scott/$SCOTTPASS @myscript`
- **Option 1:**
  - `sqlplus /nolog @myscript`
  - *(Inside myscript)* `connect scott/tiger`
- **Option 2:**
  - `sqlplus /nolog << EOF`
  - `connect scott/tiger`
  - `EOF`
Password File

• Create a passwords file “.passwords”
  scott  tiger
  arup  aruppass

• Create a shell script “.getpass.sh”
  fgrep $1 $HOME/tools/.passwords | cut -d " " -f2

• Use it in scripts
  .getpass.sh scott | sqlplus -s scott @script.sql

© Arup Nanda, 2007
Other Options

- Use DBMS_JOB or DBMS_SCHEDULER
  - No password is ever entered or displayed
  - Jobs start only when the database is up
- Use OPS$ Accounts
  SQL> create user OPS$SCOTT identified externally;
  $ su - scott
  $ sqlplus /
- In RMAN scripts
  Old: rman target=/ rcvcat=u/p@catdb
  New: rman target=/
       connect catalog u/p@catdb
Users with Default Passwords

- About Oracle Passwords
  - PASSWORD in DBA_USERS is a hash value of the combined value of USERID and PASSWORD.
  - So even if two users have the same password, the hash value will be different.

<table>
<thead>
<tr>
<th>UserID</th>
<th>Password</th>
<th>Password Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>DEF</td>
<td>016811C1486D026B</td>
</tr>
<tr>
<td>ABCD</td>
<td>EF</td>
<td>016811C1486D026B</td>
</tr>
</tbody>
</table>

In Oracle 11g, a new view DBA_USERS_WITH_DEFPWD shows users with default passwords.
Identify Default Passwords

Create a table to hold the passwords. Script: cr OSP accounts.sql

```
CREATE TABLE OSP_ACCOUNTS
    (product VARCHAR2(30),
     security_level NUMBER(1),
     username VARCHAR2(30),
     password VARCHAR2(30),
     hash_value VARCHAR2(30),
     commentary VARCHAR2(200)
    );
```

Download the scripts from http://www.petefinnigan.com/default/osp_accounts_public.zip

Script: osp install data.sql

Then execute script get def pwd.sql

```
col password format a20
col account_status format a20
col username format a15
select o.username, o.password, d.account_status
from dba_users d, osp_accounts o
where o.hash_value = d.password;
```
Trim Privileges

• “Sweeping” Privileges
• “ANY” privileges,
  – CREATE ANY TABLE/PROCEDURE/INDEX, etc.
  – RESTRICTED SESSION
  – SELECT ANY TABLE
  – SELECT ANY DICTIONARY
  – UNLIMITED TABLESPACE
  – Script sweeping.sql
Seemingly Innocuous Privileges

• SCOTT needs to use these statements in a regular day’s work:
  – alter session set query_rewrite_enabled = true
  – alter session set optimizer_mode = …
  – alter session set sort_area_size = …
• Does SCOTT need ALTER SESSION privilege?
• NO! Alter Session System Privilege
  – is not required to change session params
  – Only required for I/O operations, e.g. trace file
  – Script – alter_sess_grantees.sql
Other Dangerous Privilages

• Create ANY Directory
  – can create a directory on any directory owned by Oracle user, incl. datafiles.

• Create ANY Trigger
  – can create triggers on any schema to capture sensitive data during insert/update

• Create Database Link
Dangerous Supplied Packages

- **UTL_TCP**
  - Main attack vehicle for the “Voyager” worm!
- **DBMS_SCHEDULER**
  - Can cause DoS attacks by calling the executables
- **DBMS_JAVA**
  - Can cause system hijacking by calling java programs to execute with oracle’s OS privs
- **UTL_FILE**
  - Can open/close files, even if controlled.
- **DBMS_ASSERT**
  - Can be used by hackers to make a user the DBA

© Arup Nanda, 2007
• Is it set to "*"?
  – Then someone can write a PL/SQL program to read (and \textbf{WRITE!}) \textbf{any} file owned by oracle, including data files, archived log files, etc.

• Use DIRECTORY objects, instead.

  \texttt{SQL> create directory MYDIR as '/u10/mydir';}
  \texttt{utl_file.fopen ('MYDIR', 'myfile.txt', 'W')}

• Revoke CREATE ANY DIRECTORY from PUBLIC

• Log Miner Dictionary File creation still needs this!

  \texttt{utl_file_dir = '/tmp'}

• Database restart required.
OS Authentication

- **OS Authenticated Users**
  
  ```
  create user OPS$JOHNUNIX identified externally;
  $ sqlplus /
  ```

- **Initialization Parameter Controls the Prefix**

  ```
  os_authentic_prefix = 'OPS$'
  ```

- **Dual Authentication**

  ```
  create user OPS$JOHNUNIX identified by JOHNPASS;
  $ sqlplus ops$johnunix/johnpass  -> not johnunix
  $ sqlplus /  -> johnunix
  ```
Indirect Grants

What will happen to ANDY’s access to TAB1 when user MARY is dropped?

GRANT SELECT ON TAB1 TO MARY WITH GRANT OPTION;

GRANT SELECT ON JOHN.TAB1 TO ANDY;

script ind_demo.sql
Effect of Indirect Grants

• Different Syntax for Different Privileges
  – System Privileges
    ```
grant create trigger to mary with admin option;
```
  – Object Privileges
    ```
grant select on tab1 to mary with grant option;
```

• If mary grants these two privileges to andy, and then mary is dropped, andy will:
  – Lose the object privileges
  – Retain the system privilege
Identify Indirect Grants

- Use script indirect_grants.sql

```sql
select grantee, privilege, owner, table_name
from dba_tab_privs
where grantor != owner;
```
Identifying Grantable Grants

Script grantable_privs_obj.sql

```sql
select grantee, owner, table_name, privilege, grantor
from dba_tab_privs
where grantable = 'YES'
and grantee != 'SYS';
```

Script grantable_privs_sys.sql

```sql
select grantee, privilege
from dba_sys_privs
where admin_option = 'YES'
and grantee not in ('SYS','DBA')
order by 1,2;
```
Simple Audit

• As a best practice, always set the database parameter AUDIT_TRAIL to DB_EXTENDED or at least DB, even if you do not want to audit anything yet.

• Oracle 11g already has it

• Objective:
  – Which user connected, OS User
  – Other details – terminal, (dis)connection time, etc.

• Auditing is expensive; so start small: audit session
Reporting

• Use this for reporting

```sql
select
to_char(timestamp, 'mm/dd/yy hh24:mi:ss') li,
  username,
os_username,
  userhost,
terminal,
to_char(logoff_time, 'mm/dd/yy hh24:mi:ss') lo
from dba_audit_trail
where logoff_time is not null;
```

• Shows who, OS user, terminal, time of login and logout

Simple_audit.sql

© Arup Nanda, 2007
Use of Simple Auditing

• Build a profile of database access
  – Which users connect, how often
  – Where they connect from, how frequently
  – How many app servers are present
  – Who is a heavy-hitter

• Prepare a Baseline

• Check regularly against the baseline to see patterns
Identify Access Violations

• Who tried but was not successful
  ```sql
  select username, os_username, terminal, userhost,
     to_char(timestamp, 'mm/dd/yy hh24:mi:ss') logon_ts
  from dba_audit_trail
  where returncode = 1017;  
  ```  
  Unsucc.sql

• Was someone trying to “guess” userids?
  ```sql
  select username from dba_audit_trail
  where returncode = 1017  
  minus
  select username from dba_users;  
  ```  
  Wrong.sql

© Arup Nanda, 2007
Fringe Benefits

- CPU and IO Usage
  - Useful for Resource Manager/Profiles
  - Diagnosis of past performance issues
  - Capacity Planning

```sql
select username, to_char(logoff_time,'mm/dd') ts,
    count(1) cnt,
    sum(session_cpu) sum_cpu,
    avg(session_cpu) avg_cpu,
    min(session_cpu) min_cpu,
    max(session_cpu) max_cpu
from dba_audit_trail
group by username, to_char(logoff_time,'mm/dd')
order by username, to_char(logoff_time,'mm/dd')
```
Auditing on Objects

• By Access
  – `audit select on ccmaster.credit_cards by access;`
  – One record per access

• By Session
  – `audit select on ccmaster.credit_cards by session;`
  – One record per session
Object Audit by Session

```
select username, timestamp, ses_actions
from dba_audit_trail
where obj_name = 'CREDIT_CARDS'
and action_name = 'SESSION REC';
```

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>TIMESTAMP</th>
<th>SES_ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARUP</td>
<td>16-JAN-06</td>
<td>S------------</td>
</tr>
</tbody>
</table>

(sessaud.sql)
# SES_ACTIONS

<table>
<thead>
<tr>
<th>Position</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alter</td>
</tr>
<tr>
<td>2</td>
<td>Audit</td>
</tr>
<tr>
<td>3</td>
<td>Comment</td>
</tr>
<tr>
<td>4</td>
<td>Delete</td>
</tr>
<tr>
<td>5</td>
<td>Grant</td>
</tr>
<tr>
<td>6</td>
<td>Index</td>
</tr>
<tr>
<td>7</td>
<td>Insert</td>
</tr>
<tr>
<td>8</td>
<td>Lock</td>
</tr>
<tr>
<td>9</td>
<td>Rename</td>
</tr>
<tr>
<td>10</td>
<td>Select</td>
</tr>
<tr>
<td>11</td>
<td>Update</td>
</tr>
<tr>
<td>12</td>
<td>References</td>
</tr>
<tr>
<td>13</td>
<td>Execute</td>
</tr>
<tr>
<td>14</td>
<td>Not used</td>
</tr>
<tr>
<td>15</td>
<td>Not used</td>
</tr>
<tr>
<td>16</td>
<td>Not used</td>
</tr>
</tbody>
</table>

S – for Success; F – for Failure and B – for Both
Object Auditing by Access

```sql
select to_char(timestamp,'mm/dd/yy hh24:mi:ss') ts,
       username, userhost, action_name
from dba_audit_trail
where owner = 'CCMASTER'
and obj_name = 'CREDIT_CARDS';
```

<table>
<thead>
<tr>
<th>TS</th>
<th>USERNAME</th>
<th>USERHOST</th>
<th>ACTION_NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/16/06 00:27:44</td>
<td>ARUP</td>
<td>prolin1</td>
<td>SELECT</td>
</tr>
<tr>
<td>01/16/06 11:03:24</td>
<td>ARUP</td>
<td>prolin1</td>
<td>UPDATE</td>
</tr>
<tr>
<td>01/16/06 12:34:00</td>
<td>ARUP</td>
<td>prolin1</td>
<td>SELECT</td>
</tr>
</tbody>
</table>
Thoughts on Auditing Use

- Set the initialization parameter `audit_trail = db or db_extended`
- Start with BY SESSION, dig deeper into BY ACCESS later
- Find attempted break-ins by auditing for unsuccessful attempts:
  - `audit select on CCMASTER.CREDIT_CARDS by session whenever not successful;`
Control Schema Changes

• Problem:
  – ACCMAN; main schema. password known to the application group
  – ACCAPP: the user that connects to the database.
  – How do you ensure that the DDL changes are in tune with the Change Management Process?

• Solution:
  – Release Manager: Unlocks “something”
  – App DBA/Developer: Makes the DDL change
  – Release Manager: Locks “it”; no DDL allowed
DDL Triggers `lock_alter.sql`

```sql
1  create or replace trigger lock_alter
2    before ddl
3    on accman.schema
4    begin
5      if (  
6        ora_dict_obj_name = 'IMPORTANT_PROC'
7        and
8        ora_sysevent = 'CREATE'
9      ) 
10     then
11        raise_application_error
12          (-20001, 'Can't Alter ' || ora_dict_obj_name);
13      end if;
14    end;
```

“Unlock” : `alter trigger lock_alter disable;`

```
alter_imp_proc.sql
```

© Arup Nanda, 2007
Listener Log Monitoring

- Listener Log records the connections from
- For a complete description, including code and examples, see:
  http://www.dbazine.com/oracle/or-articles/nanda14
Plan

- Make listener changes
- Reload listener to take effect
- Make all nonrequired binary changes
- Make all binary permission changes
- Make the changes to the INIT.ORA params
- Recycle the database
- Remove Sweeping Privileges
- Remove Execute Privileges from PUBLIC
Thank You!

Download Scripts, Presentations from http://www.proligence.com

Questions?

© Arup Nanda, 2007