Logica Guru4Pro

June 2nd 2010

Oracle Security

The Right Approach (IMHO)

By

Pete Finnigan

Updated Friday, 21st May 2010

Why Am I Qualified To Speak

- PeteFinnigan.com Ltd, Est 2003.
- http://www.petefinnigan.com
- First “Oracle security” blog.
- Specialists in researching and securing Oracle databases providing consultancy and training Database scanner software authors and vendors.
- Author of Oracle security step-by-step book; co-author of Expert Oracle practices, author of HSM/TDE Book to be published soon.
- Published many papers, regular speaker (UK, USA, Slovenia, Norway, Iceland, Finland and more).
- Member of the Oak Table Network.

Agenda

- Background “glue”
- The correct approach (IMHO) – The message
- Exploit + reaction (a number of levels)
  - downloadable, easy
  - Realistic theft
  - Sophisticated attack
  - Data analysis
  - User Analysis
- Conclusions

Introduction

- You have me for 2 hours (or longer, I am flexible)
  - The focus is "***how easy it is to steal***" [some examples] and "***how easy it is to not secure properly***" [examples]
  - But i want to give you some
  - And; we are going to try a lot of demos!

Overview

- What do I want to achieve this evening
  - I want you to “grasp” some of the basic ideas behind securing an Oracle database – I will say what they are at the end BUT see if you can pick them up
- Anyone can secure an Oracle database BUT we should get the ground rules right and really understand why to secure and how to secure
- **Ask questions any time you would like to**
- Try out some of the tools and techniques yourself later on or now if you have a local Oracle database on a laptop (NOT ALL OF THEM ON PRODUCTION!)

What Is Oracle Security?

- Securely configuring an existing Oracle database?
- Designing a secure Oracle database system before implementation for new databases?
- Understanding what you have – perform an audit?
- Using some of the key security features
  - Audit facilities, encryption functions, RBAC, FGA, VPD…
- Oracle security is about all of these BUT
  - **It is about securely storing critical / valuable data in an Oracle database. In other words its about securing DATA not securing the software!**

Traditional Security Approach

- Hardening by checklist – good idea?
- A number of them available
  - SANS Step-by-step guide
  - SANS S.C.O.R.E.
  - CIS benchmark
  - DoD Stig
  - IT Governance book
  - Oracle’s own checklist

Problems With Checklists

- Not many checklists exist for Oracle databases
- Most are from same initial source or are very similar
- Some structure there but not good enough
  - “tip based rather than method based”
- Lists don’t focus on securing the data
- Difficult to implement for a large number of databases
- CIS for instance has 158 pages

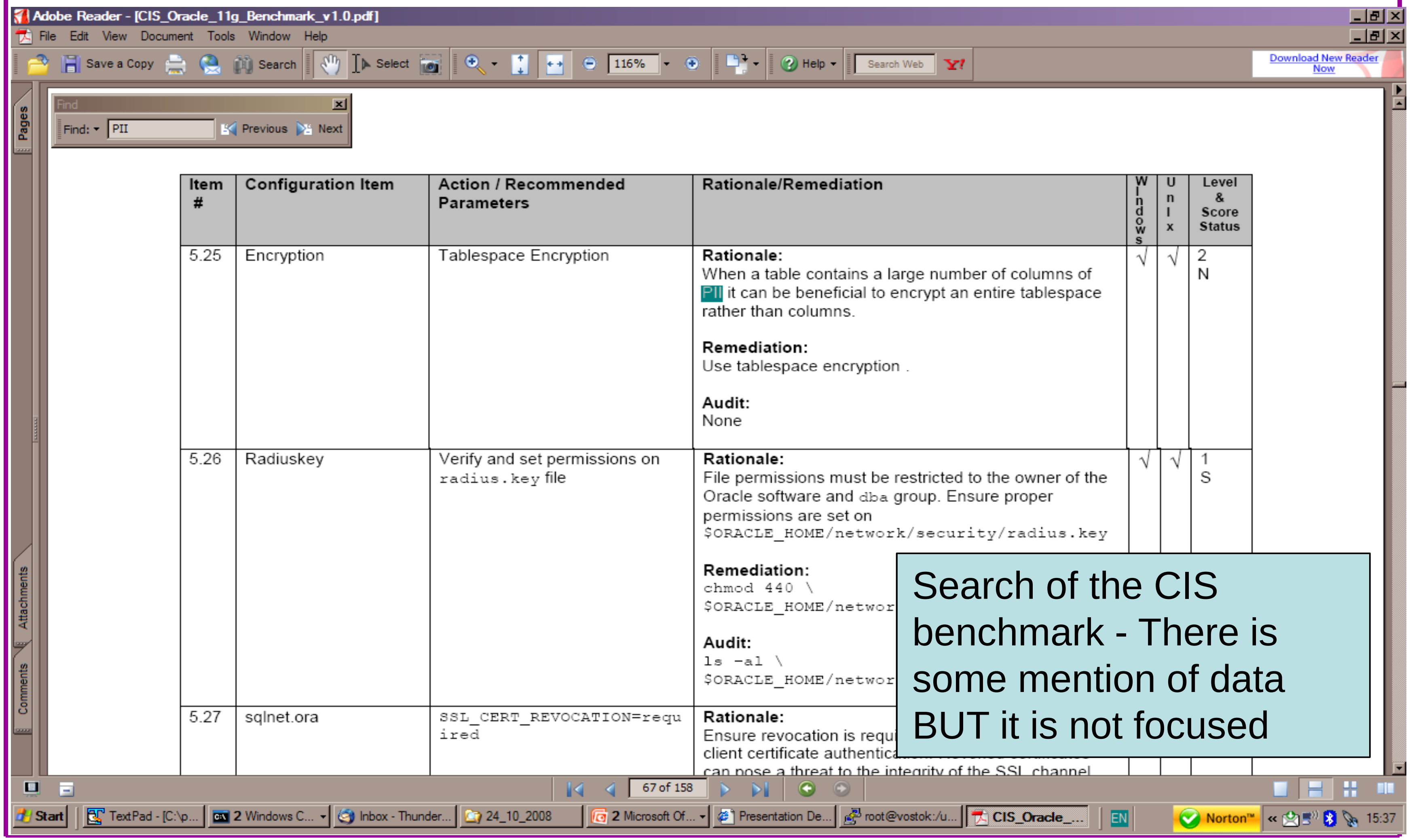
Solutions are not Simple

- Time based solution
  - Could spend man years on even a single database
  - Finding solutions for each issue is not as simple as applying what it says in the document
- Clever solutions are needed
  - Technical solutions need to be specified
  - Onion based approach is good
  - Basic hardening in parallel

Examples Of Problems

- Two examples:
  1) Check 3.0.2 in CIS states “all files in $ORACLE_HOME/bin directory must have privileges of 0755 or less – fine - but the solution states “chmod 0755 $ORACLE_HOME/bin/*” – is it a good idea?
  2) Solutions are not as simple as indicated. For instance fixing a weak password should also include, fix the password, management, hard coded passwords, audit, policy….

Checklists And PII Data



Find: PII

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
5.25	Encryption	Tablespace Encryption	**Rationale:** When a table contains a large number of columns of PII it can be beneficial to encrypt an entire tablespace rather than columns. **Remediation:** Use tablespace encryption . **Audit:** None	√	√	2 N

5.26	Radiuskey	Verify and set permissions on `radius.key` file	**Rationale:**
			File permissions must be restricted to the owner of the Oracle software and `dba` group. Ensure proper permissions are set on `$ORACLE_HOME/network/security/radius.key`
			Remediation:
			`chmod 440 \`
			`$ORACLE_HOME/networ`
			Audit:
			`ls -al \`
			`$ORACLE_HOME/networ`
				√	√	1
						S

5.27	sqlnet.ora	`SSL_CERT_REVOCATION=required`	**Rationale:** Ensure revocation is requi client certificate authentica can pose a threat to the integrity of the SSL channel			

Search of the CIS benchmark - There is some mention of data BUT it is not focused

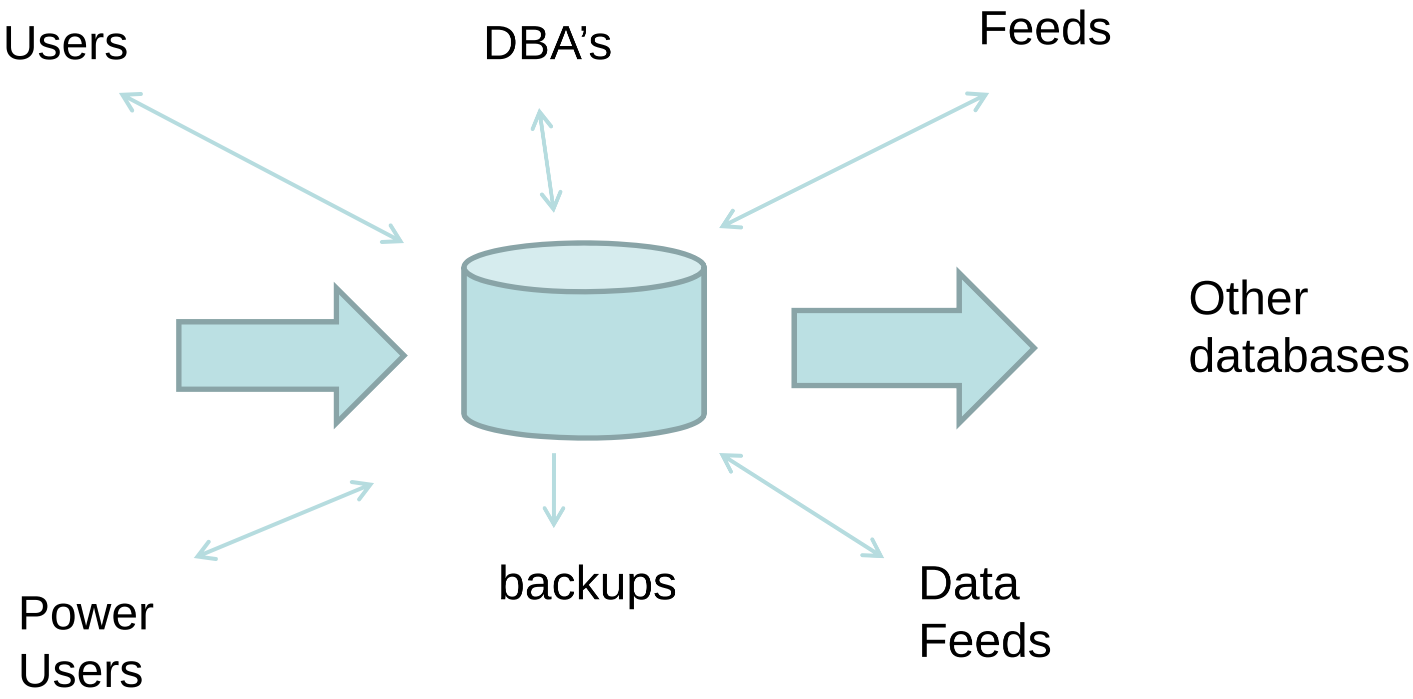
The Right Method To Secure

- Start with “**the data**”
- Understand “**data flow**” and “**access**”
- Understand the problem of securing “**your data**”
- Hardening should be part of the solution **BUT** not **THE** solution
- Checklists do not mention “**your**” data

Complex But Simple Solutions Needed

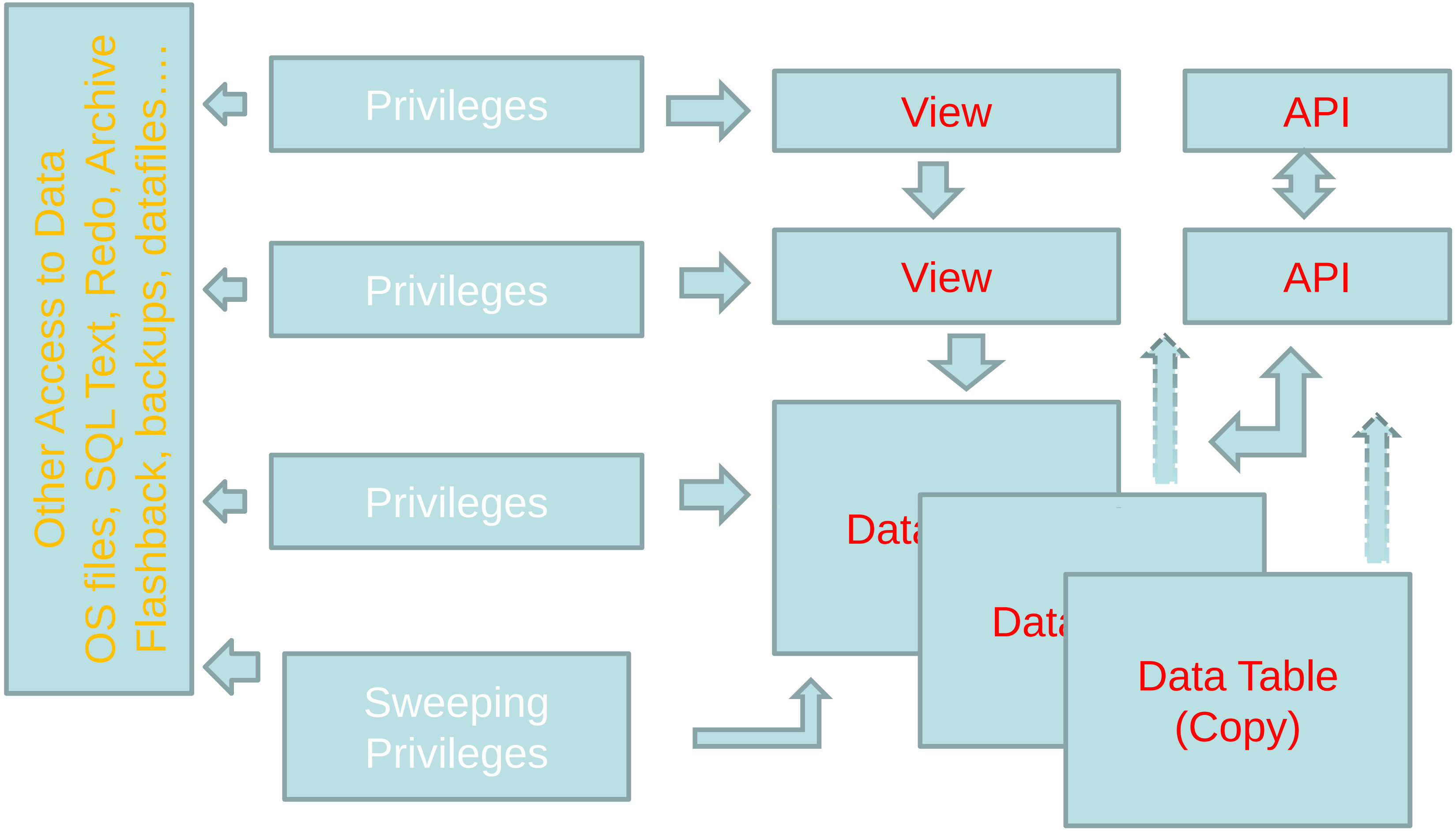
- Overarching solutions are needed
- Remove all types of access from the data
- Ensure only those who should see, can see the data
- Unfortunately it’s not that simple as there are:
  - Many paths to the data
  - Many copies of data
  - Data stored or in transit that is accessible
  - Data copied outside of the database

Understand Architecture



Identify each type of person and a sample account for each

Data Access Models



Data Access Is Not “Flat”

- Data model is not flat – remove the “blinkers”
- Access rights are also not flat
- Data is often replicated
  - In other tables – in interfaces – flexfields …
  - Indexes
  - Shared memory
  - Data files
  - Operating system
  - Many more…

How / Who

- The data must be identified (found?)
- The access paths must be found
- The “people” – real people identified
- Map to these to database user accounts
- Assess who can access data and how
- Only now can we hope to secure data

Database Security Focus

- If you are a hacker what is the focus?
  - Lots of bugs to study
  - Lots of exploits for download
  - Lots of info on hacking Oracle to use
- If you are a defender what is the focus?
  - In my experience not much has been done
  - People rely on Oracle doing the work BUT they don’t!

More for the Attacker

- Lots of databases have these issues:
  - Weak and guessable passwords
  - No password management (fixed from 11gR1 and 10.2.0.2)
  - Weak controls on the data and functions
  - No audit in the database (fixed from 11gR1 and 10.2.0.2)
  - Weak privilege design for users, solutions (batch, feeds etc) and DBA’s
  - Usually no processes to manage any breach or potential breach

Simple Exploit

- Escalation of Privileges
- 5 minutes demonstration

Live Demo 1

What are the issues?

- For you:
  - Easy to down load
  - Easy to run
  - No skill needed
  - Everyone learn about and download
  - Only real solution is patch (for most bugs / exploits)
  - BUT.....

Payloads, Targets

- The focus of researchers is “grant DBA to public”
- This is wrong, the possible payloads are infinite
- The “real” target is
  - Data
  - Job satisfaction
  - Revenge
  - More?
- Factor in IDS evasion
- Factor in downloadable exploits benefit those who “know”...

Stealing Data - Realistic

- We are now going to demonstrate a much more realistic case of simple data theft
- This is more realistic because real systems audited by us allow this to happen – indeed we know theft using techniques like this has happened

Breach - Slide 2

- Hacking an Oracle database to “steal”
- 15 minutes demonstration

Live Demo 2

Reaction

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

Some Issues?

- OK, easy and realistic
- There are still issues, for someone to steal they still need Oracle knowledge and business knowledge
- The issue is that because “WE” (the Oracle customers) do not fix databases we make it easy to steal – the target audience for these “ADVANTAGES” is likely employees – DBA, Power users, Dev....

Data Theft

- Data theft is more likely possible due to:
  - Application abuse
  - Data not in the database
  - Data given to users
  - More....
- Oracle will not fix these issues for you, they are your responsibility!

The Defenders View

- Did our realistic attack leave evidence
- Does the DBA review these evidences?
- Audit trail
- Listener log
- redo
- More...

Live Demo 3

What if the Hacker Was Clever

- If he was clever he may take a number of different approaches
  - Stealth
    - in finding an account
    - Escalate first
    - Check identity
    - Steal the data from somewhere else

A Stealth Attack

Live Demo 4

Some Thoughts

- A data security solution must be comprehensive
- All copies of the data must be located and protected to the same level
- Theft will always occur taking the easiest approach!

The True Access To The Data

Live Demo 5

The Access Issue

- This is the number 1 Oracle security issue for me
- 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
- A database can only be accessed at the TNS level if there is a direct route from the user (authorised or not) and the database

11gR1 has broken this with the default sid/service name feature

Access Issue 2

- At lots of sites we audit we see:
  - Tnsnames.ora deployed to all servers and desktops
  - Tnsnames.ora with details of every database
  - access to servers is open (no IP blocking)
  - Guessable SID/Service name
  - Weak passwords
- Do not do any of these at your sites!

The Core Problems

- Incorrect versions and products installed
- Unnecessary functions and features installed
- Excessive users / schemas installed
- Elevated privileges for most database accounts
- Default and insecure configurations
- Lack of audit trails in the database
- Data often held outside the database
- Evidence of ad-hoc maintenance

Configuration And Defaults

- Default database installations cause some weak configurations
- Review all
  - configuration parameters – checklists?
  - File permissions
- Some examples
  - No audit configuration by default (fixed in 10gR2 for new installs)
  - No password management (fixed in 10gR2 new installs)
- In your own applications and support accounts
  - Do not use default accounts
  - Do not use default roles including DBA
  - Do not use default passwords

Background Information

- Basic information must be to hand for familiarisation rather than actual use
- 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

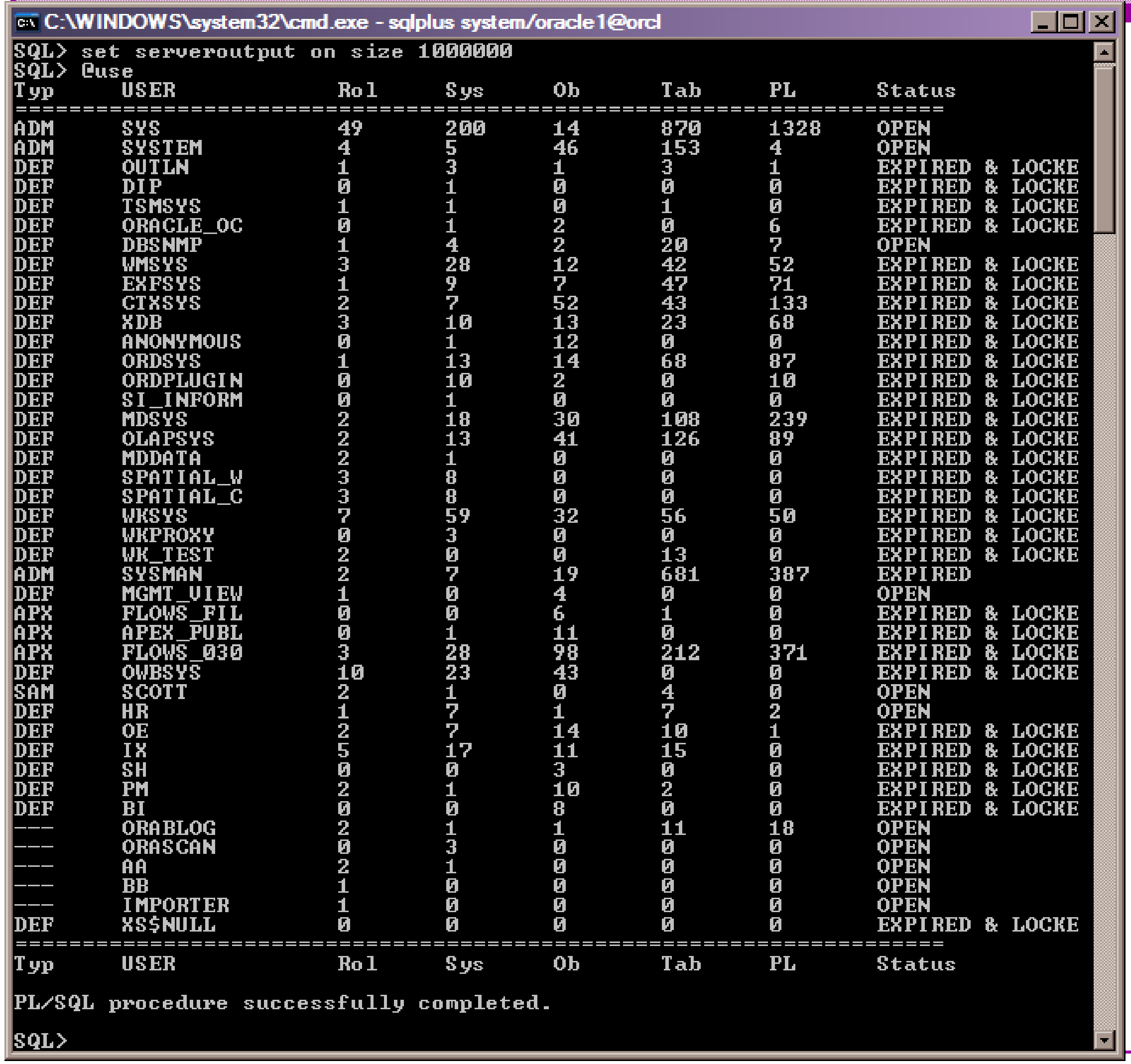
Background Information 2

- Some background information we do use!
- There are a few standalone tools available
- I would start with manual queries and toolkit of 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

Background Information 3

- 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

Analysis Of Users



```
SQL> set serveroutput on size 1000000
SQL> @use
Typ     USER            Rol     Sys     Ob      Tab     PL      Status
=====================================================================
ADM     SYS             49      200     14      870     1328    OPEN
ADM     SYSTEM          4       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     EXPIRED
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       1       0       4       0       OPEN
DEF     HR              1       7       1       7       2       OPEN
DEF     OE              2       7       14      10      1       EXPIRED & LOCKE
DEF     IX              5       17      11      15      0       EXPIRED & LOCKE
DEF     SH              0       0       3       0       0       EXPIRED & LOCKE
DEF     PM              2       1       10      2       0       EXPIRED & LOCKE
DEF     BI              0       0       8       0       0       EXPIRED & LOCKE
---     ORABLOG         2       1       1       11      18      OPEN
---     ORASCAN         0       3       0       0       0       OPEN
---     AA              2       1       0       0       0       OPEN
---     BB              1       0       0       0       0       OPEN
---     IMPORTER        1       0       0       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>
```

Analyse users into 2 groups

Seek to reduce the accounts (features) installed as default schemas – i.e. OEM, Intelligent agent, DIP, Samples

Analyse accounts created by "you". Assess these in terms of what should exist

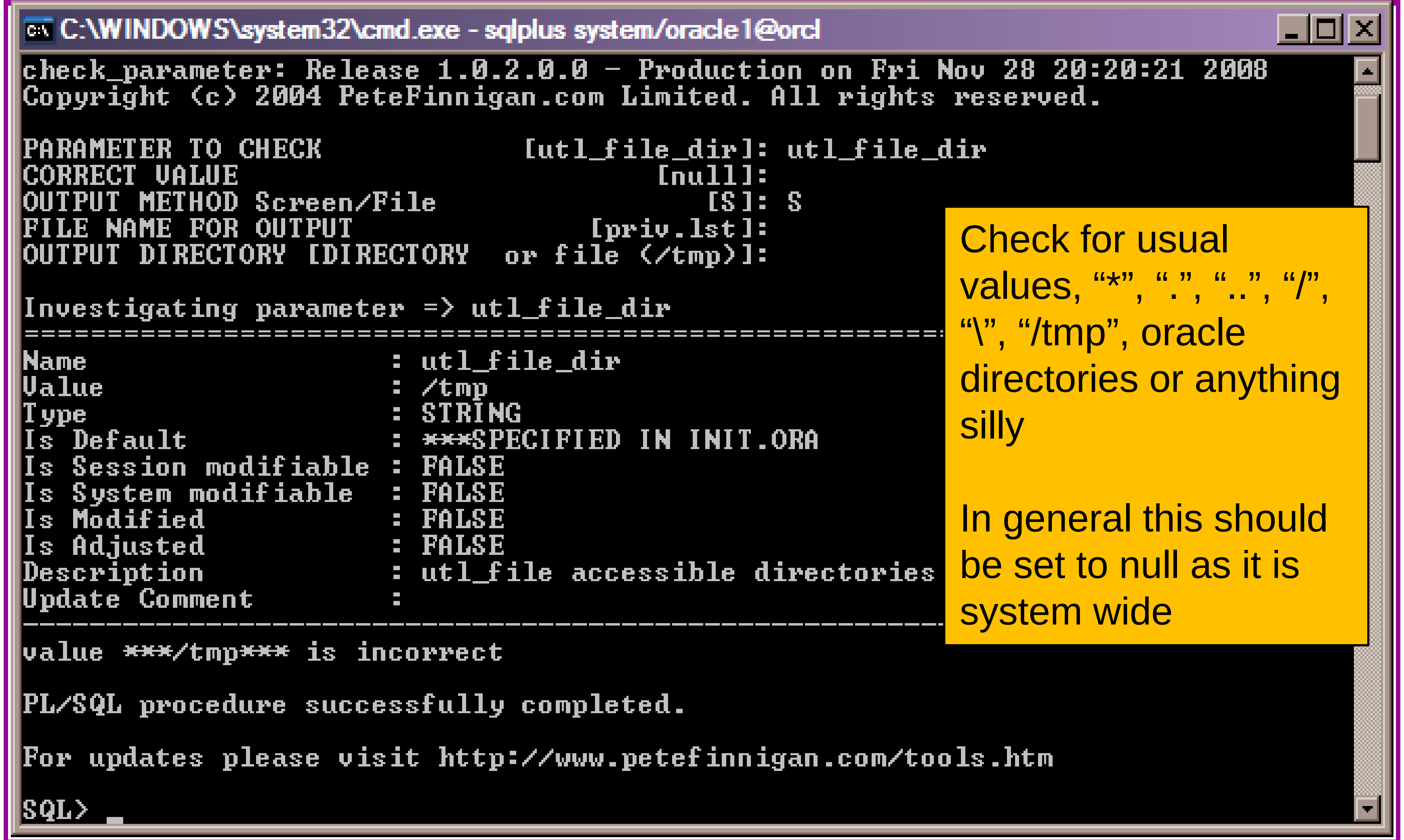
Analysing Users

Live Demo 7

Access To The Server - 1

- We are now going to investigate in depth the issues around accessing the operating system
- We should now be ready for "***layers***" and "***hierarchy***" being evident in this investigation
- We will look at the common interfaces and common procedures

Access To The Server - 2

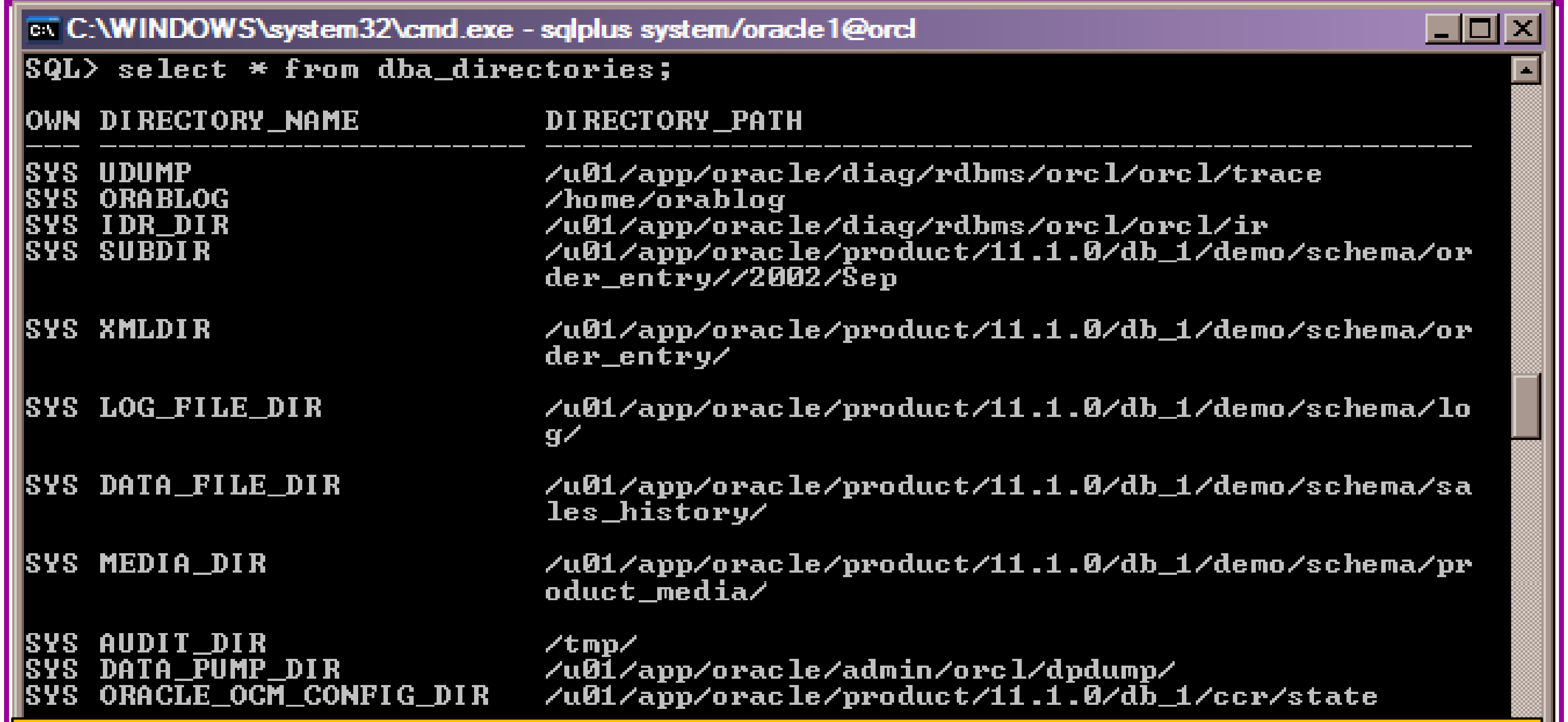


```
check_parameter: Release 1.0.2.0.0 - Production on Fri Nov 28 20:20:21 2008
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

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

Investigating parameter => utl_file_dir
=======================================================
Name                     : utl_file_dir
Value                    : /tmp
Type                     : STRING
Is Default               : ***SPECIFIED IN INIT.ORA
Is Session modifiable    : FALSE
Is System modifiable     : FALSE
Is Modified              : FALSE
Is Adjusted              : FALSE
Description              : utl_file accessible directories
Update Comment           :
-------------------------------------------------------
value ***/tmp*** is incorrect

PL/SQL procedure successfully completed.

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

SQL> _
```

Check for usual values, “*”, “.”, “..”, “/”, “\”, “/tmp”, oracle directories or anything silly

In general this should be set to null as it is system wide

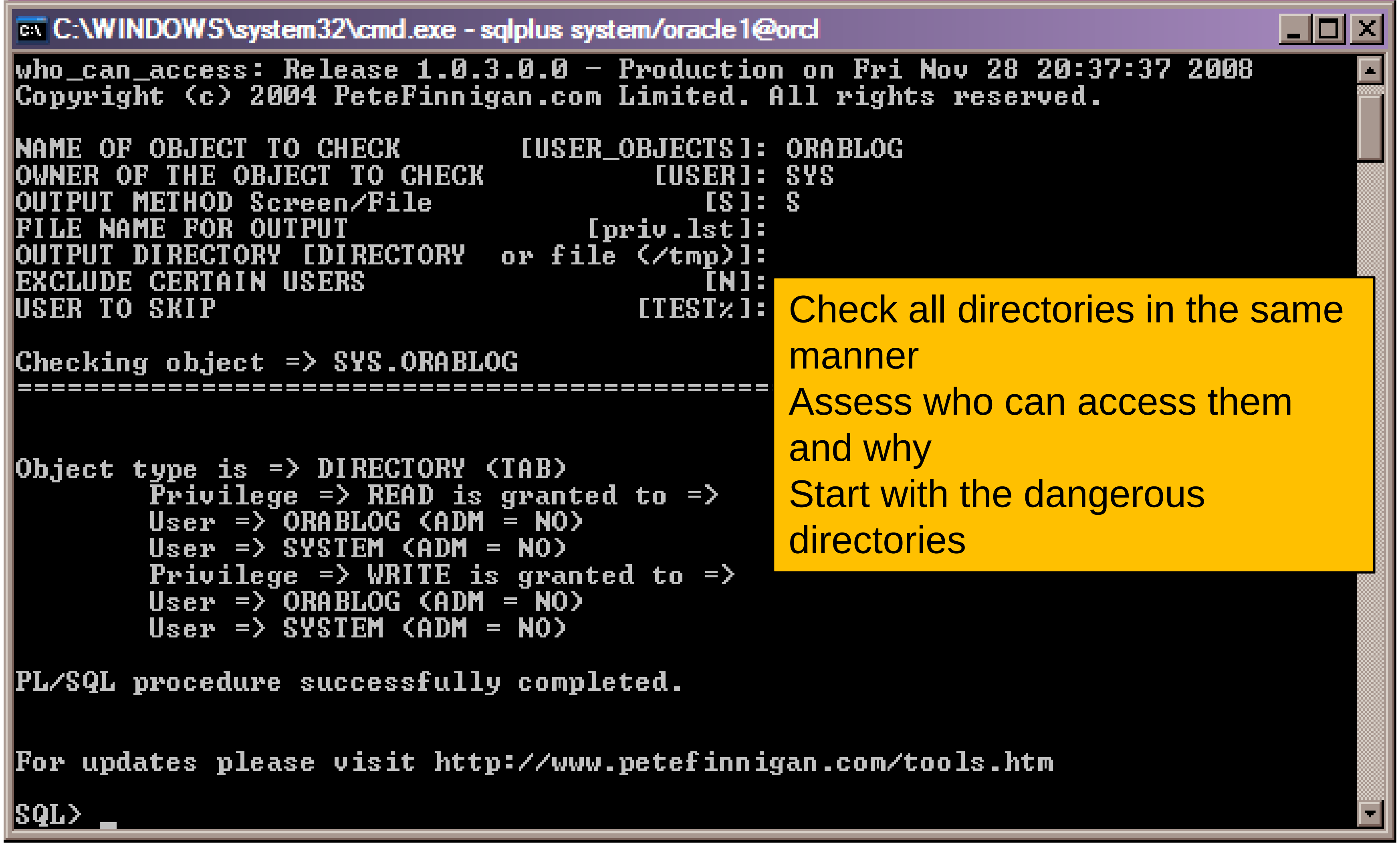
Access To The Server - 3



```
SQL> select * from dba_directories;

OWN DIRECTORY_NAME                 DIRECTORY_PATH
--- ------------------------------ --------------------------------------------------
SYS UDUMP                          /u01/app/oracle/diag/rdbms/orcl/orcl/trace
SYS ORABLOG                        /home/orablog
SYS IDR_DIR                        /u01/app/oracle/diag/rdbms/orcl/orcl/ir
SYS SUBDIR                         /u01/app/oracle/product/11.1.0/db_1/demo/schema/or
                                   der_entry//2002/Sep

SYS XMLDIR                         /u01/app/oracle/product/11.1.0/db_1/demo/schema/or
                                   der_entry/

SYS LOG_FILE_DIR                   /u01/app/oracle/product/11.1.0/db_1/demo/schema/lo
                                   g/

SYS DATA_FILE_DIR                  /u01/app/oracle/product/11.1.0/db_1/demo/schema/sa
                                   les_history/

SYS MEDIA_DIR                      /u01/app/oracle/product/11.1.0/db_1/demo/schema/pr
                                   oduct_media/

SYS AUDIT_DIR                      /tmp/
SYS DATA_PUMP_DIR                  /u01/app/oracle/admin/orcl/dpdump/
SYS ORACLE_OCM_CONFIG_DIR          /u01/app/oracle/product/11.1.0/db_1/ccr/state
```

Split the directories into two groups, those created by Oracle and those added by the customer
Look for dangerous directories, ORABLOG, UDUMP, AUDIT_DIR [default] look useful for a hacker

Access To The Server - 4



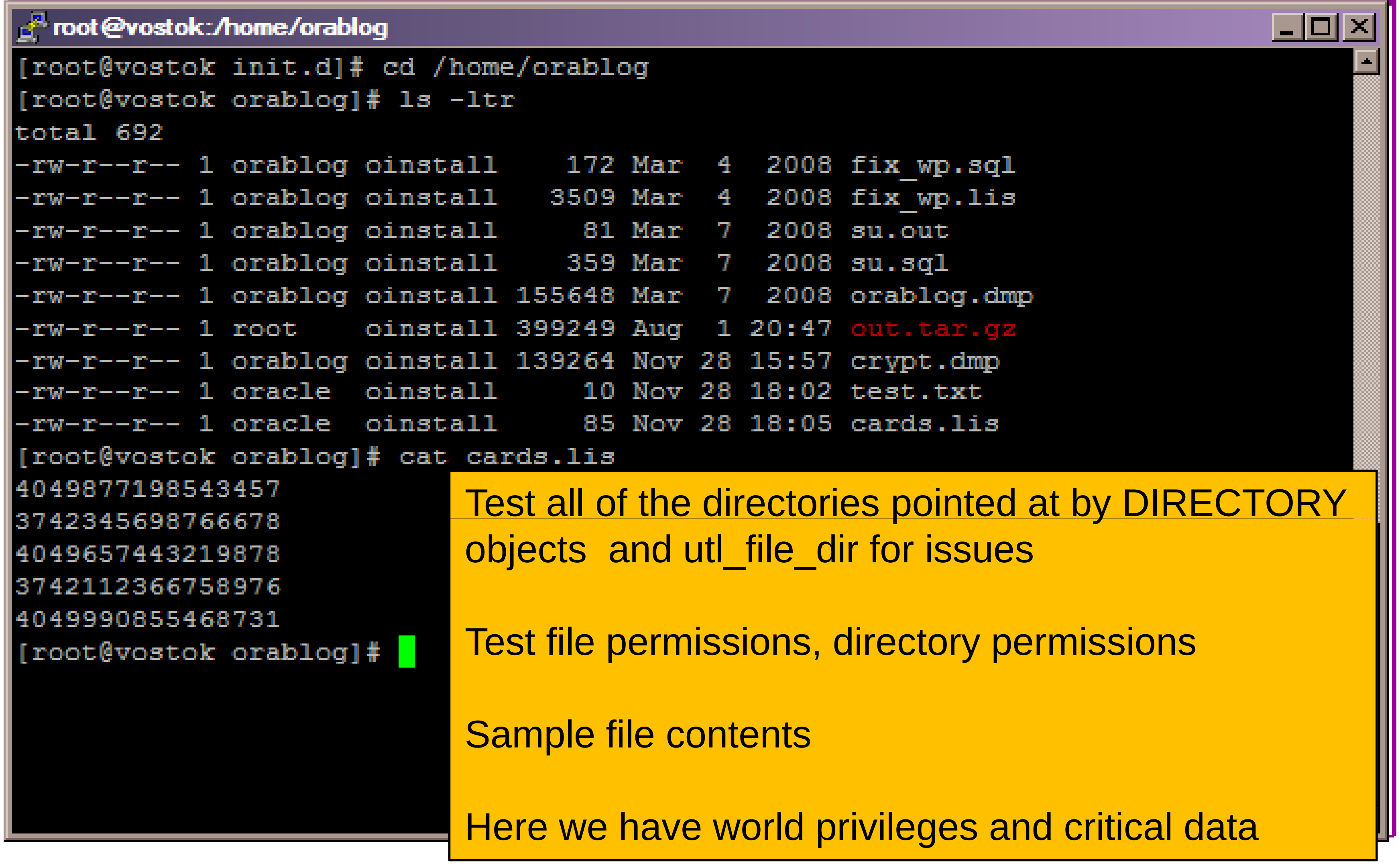
```
who_can_access: Release 1.0.3.0.0 - Production on Fri Nov 28 20:37:37 2008
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK       [USER_OBJECTS]: ORABLOG
OWNER OF THE OBJECT TO CHECK          [USER]: SYS
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%]:

Checking object => SYS.ORABLOG
=============================================


Object type is => DIRECTORY (TAB)
        Privilege => READ is granted to =>
        User => ORABLOG (ADM = NO)
        User => SYSTEM (ADM = NO)
        Privilege => WRITE is granted to =>
        User => ORABLOG (ADM = NO)
        User => SYSTEM (ADM = NO)

PL/SQL procedure successfully completed.


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

SQL> _
```

Check all directories in the same manner

Assess who can access them and why

Start with the dangerous directories

Access To The Server - 5



```
[root@vostok init.d]# cd /home/orablog
[root@vostok orablog]# ls -ltr
total 692
-rw-r--r-- 1 orablog oinstall    172 Mar  4  2008 fix_wp.sql
-rw-r--r-- 1 orablog oinstall   3509 Mar  4  2008 fix_wp.lis
-rw-r--r-- 1 orablog oinstall     81 Mar  7  2008 su.out
-rw-r--r-- 1 orablog oinstall    359 Mar  7  2008 su.sql
-rw-r--r-- 1 orablog oinstall 155648 Mar  7  2008 orablog.dmp
-rw-r--r-- 1 root    oinstall 399249 Aug  1 20:47 out.tar.gz
-rw-r--r-- 1 orablog oinstall 139264 Nov 28 15:57 crypt.dmp
-rw-r--r-- 1 oracle  oinstall     10 Nov 28 18:02 test.txt
-rw-r--r-- 1 oracle  oinstall     85 Nov 28 18:05 cards.lis
[root@vostok orablog]# cat cards.lis
4049877198543457
3742345698766678
4049657443219878
3742112366758976
4049990855468731
[root@vostok orablog]# 
```

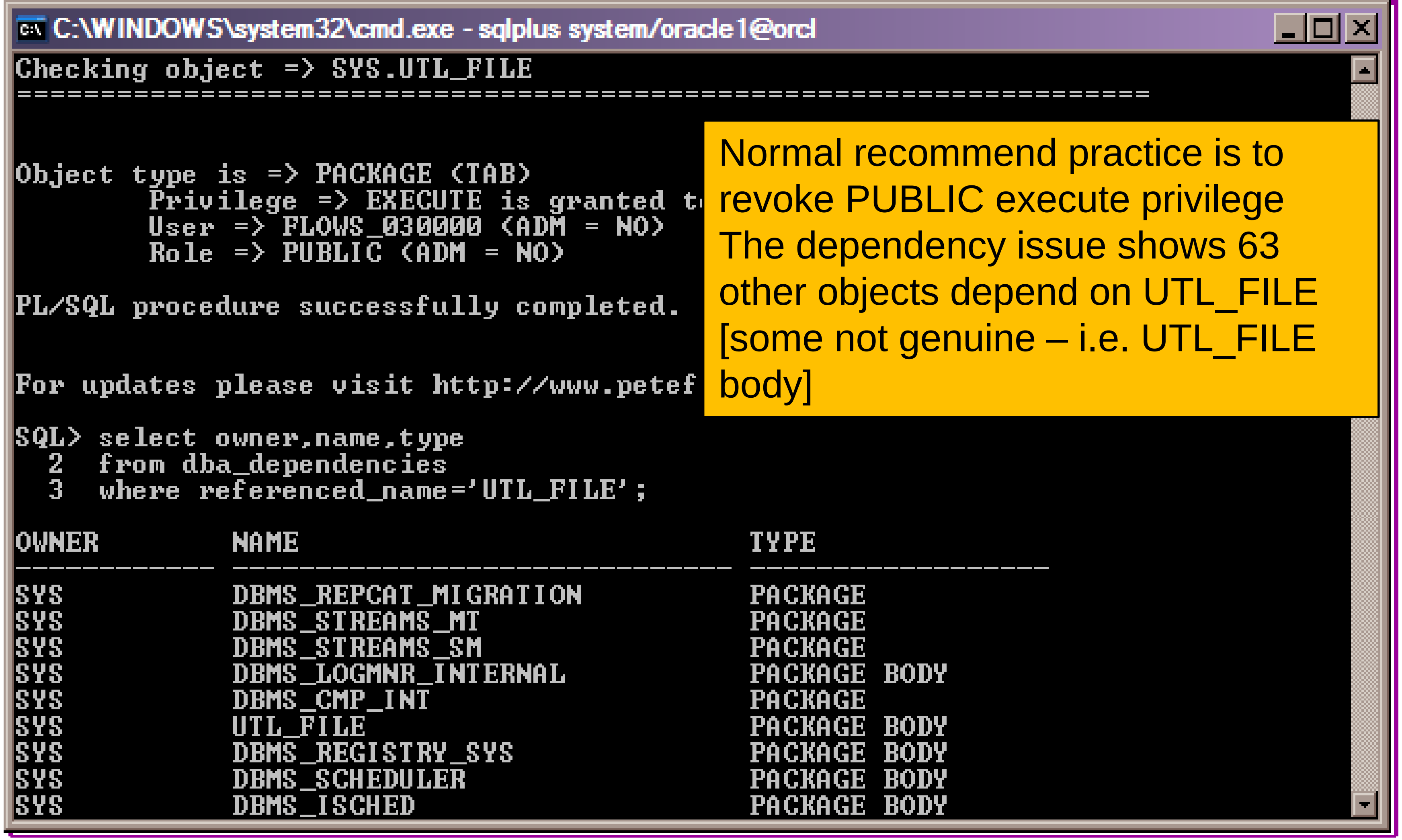
Test all of the directories pointed at by DIRECTORY objects and utl_file_dir for issues

Test file permissions, directory permissions

Sample file contents

Here we have world privileges and critical data

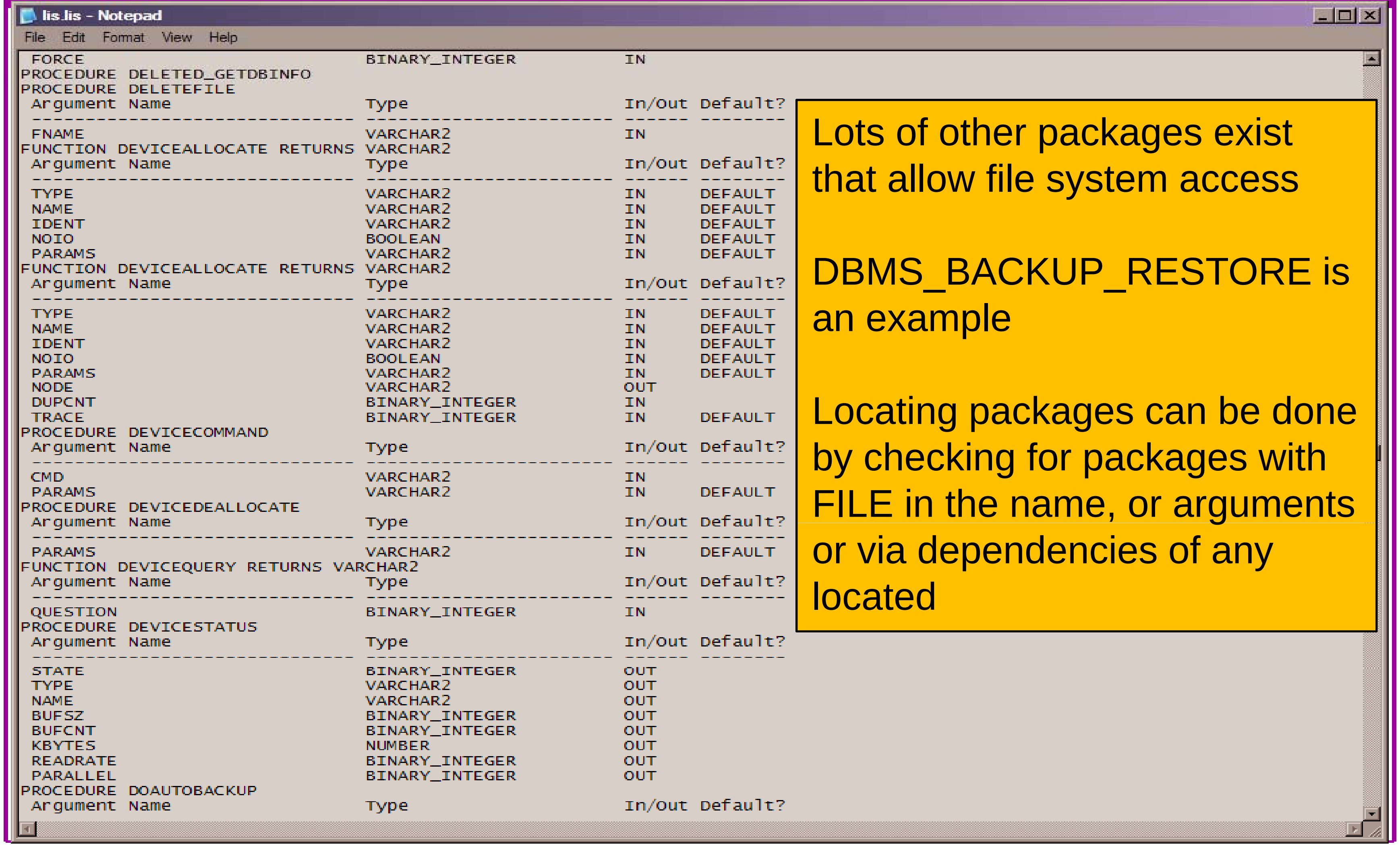
Access To The Server - 6



```
Checking object => SYS.UTL_FILE
====================================================================


Object type is => PACKAGE (TAB)
        Privilege => EXECUTE is granted t
        User => FLOWS_030000 (ADM = NO)
        Role => PUBLIC (ADM = NO)

PL/SQL procedure successfully completed.


For updates please visit http://www.petef

SQL> select owner,name,type
  2  from dba_dependencies
  3  where referenced_name='UTL_FILE';

OWNER        NAME                           TYPE
------------ ------------------------------ ------------------
SYS          DBMS_REPCAT_MIGRATION          PACKAGE
SYS          DBMS_STREAMS_MT                PACKAGE
SYS          DBMS_STREAMS_SM                PACKAGE
SYS          DBMS_LOGMNR_INTERNAL           PACKAGE BODY
SYS          DBMS_CMP_INT                   PACKAGE
SYS          UTL_FILE                       PACKAGE BODY
SYS          DBMS_REGISTRY_SYS              PACKAGE BODY
SYS          DBMS_SCHEDULER                 PACKAGE BODY
SYS          DBMS_ISCHED                    PACKAGE BODY
```

Normal recommend practice is to revoke PUBLIC execute privilege The dependency issue shows 63 other objects depend on UTL_FILE [some not genuine – i.e. UTL_FILE body]

Access To The Server - 7



```
 FORCE                          BINARY_INTEGER          IN
PROCEDURE DELETED_GETDBINFO
PROCEDURE DELETEFILE
 Argument Name                  Type                    In/Out Default?
 ------------------------------ ----------------------- ------ --------
 FNAME                          VARCHAR2                IN
FUNCTION DEVICEALLOCATE RETURNS VARCHAR2
 Argument Name                  Type                    In/Out Default?
 ------------------------------ ----------------------- ------ --------
 TYPE                           VARCHAR2                IN     DEFAULT
 NAME                           VARCHAR2                IN     DEFAULT
 IDENT                          VARCHAR2                IN     DEFAULT
 NOIO                           BOOLEAN                 IN     DEFAULT
 PARAMS                         VARCHAR2                IN     DEFAULT
FUNCTION DEVICEALLOCATE RETURNS VARCHAR2
 Argument Name                  Type                    In/Out Default?
 ------------------------------ ----------------------- ------ --------
 TYPE                           VARCHAR2                IN     DEFAULT
 NAME                           VARCHAR2                IN     DEFAULT
 IDENT                          VARCHAR2                IN     DEFAULT
 NOIO                           BOOLEAN                 IN     DEFAULT
 PARAMS                         VARCHAR2                IN     DEFAULT
 NODE                           VARCHAR2                OUT
 DUPCNT                         BINARY_INTEGER          IN
 TRACE                          BINARY_INTEGER          IN     DEFAULT
PROCEDURE DEVICECOMMAND
 Argument Name                  Type                    In/Out Default?
 ------------------------------ ----------------------- ------ --------
 CMD                            VARCHAR2                IN
 PARAMS                         VARCHAR2                IN     DEFAULT
PROCEDURE DEVICEDEALLOCATE
 Argument Name                  Type                    In/Out Default?
 ------------------------------ ----------------------- ------ --------
 PARAMS                         VARCHAR2                IN     DEFAULT
FUNCTION DEVICEQUERY RETURNS VARCHAR2
 Argument Name                  Type                    In/Out Default?
 ------------------------------ ----------------------- ------ --------
 QUESTION                       BINARY_INTEGER          IN
PROCEDURE DEVICESTATUS
 Argument Name                  Type                    In/Out Default?
 ------------------------------ ----------------------- ------ --------
 STATE                          BINARY_INTEGER          OUT
 TYPE                           VARCHAR2                OUT
 NAME                           VARCHAR2                OUT
 BUFSZ                          BINARY_INTEGER          OUT
 BUFCNT                         BINARY_INTEGER          OUT
 KBYTES                         NUMBER                  OUT
 READRATE                       BINARY_INTEGER          OUT
 PARALLEL                       BINARY_INTEGER          OUT
PROCEDURE DOAUTOBACKUP
 Argument Name                  Type                    In/Out Default?
```

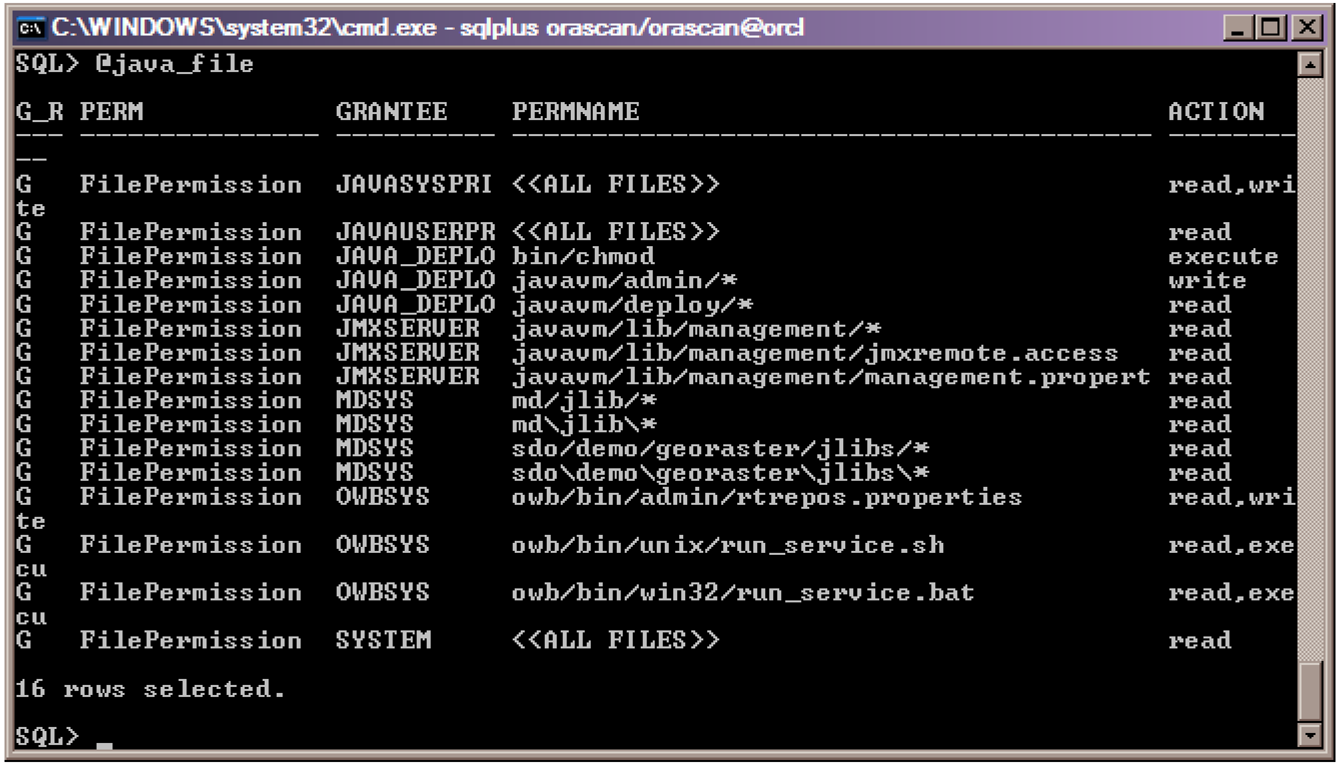
Lots of other packages exist that allow file system access

DBMS_BACKUP_RESTORE is an example

Locating packages can be done by checking for packages with FILE in the name, or arguments or via dependencies of any located

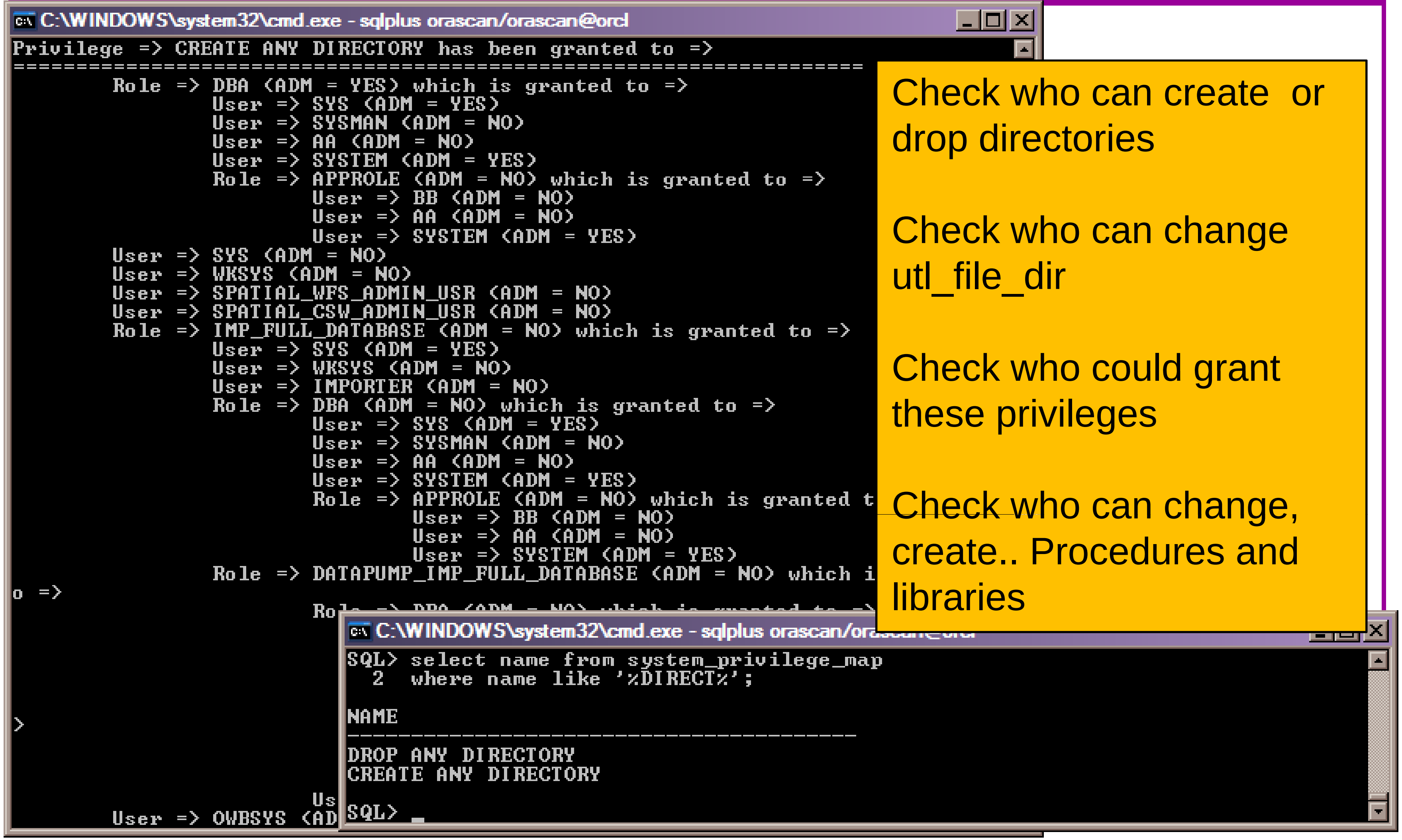
Access To The Server - 8

- Java – find file access permissions
- Locate all packages that use the privileges, check dependencies, access to those packages…



```
SQL> @java_file

G_R PERM            GRANTEE    PERMNAME                                 ACTION
--- --------------- ---------- ---------------------------------------- --------
--
G   FilePermission  JAVASYSPRI <<ALL FILES>>                            read,wri
te
G   FilePermission  JAVAUSERPR <<ALL FILES>>                            read
G   FilePermission  JAVA_DEPLO bin/chmod                                execute
G   FilePermission  JAVA_DEPLO javavm/admin/*                           write
G   FilePermission  JAVA_DEPLO javavm/deploy/*                          read
G   FilePermission  JMXSERVER  javavm/lib/management/*                  read
G   FilePermission  JMXSERVER  javavm/lib/management/jmxremote.access   read
G   FilePermission  JMXSERVER  javavm/lib/management/management.propert read
G   FilePermission  MDSYS      md/jlib/*                                read
G   FilePermission  MDSYS      md\jlib\*                                read
G   FilePermission  MDSYS      sdo/demo/georaster/jlibs/*               read
G   FilePermission  MDSYS      sdo\demo\georaster\jlibs\*               read
G   FilePermission  OWBSYS     owb/bin/admin/rtrepos.properties         read,wri
te
G   FilePermission  OWBSYS     owb/bin/unix/run_service.sh              read,exe
cu
G   FilePermission  OWBSYS     owb/bin/win32/run_service.bat            read,exe
cu
G   FilePermission  SYSTEM     <<ALL FILES>>                            read

16 rows selected.

SQL> _
```

Access To The Server - 9



```
Privilege => CREATE ANY DIRECTORY has been granted to =>
====================================================================
        Role => DBA (ADM = YES) which is granted to =>
                User => SYS (ADM = YES)
                User => SYSMAN (ADM = NO)
                User => AA (ADM = NO)
                User => SYSTEM (ADM = YES)
                Role => APPROLE (ADM = NO) which is granted to =>
                        User => BB (ADM = NO)
                        User => AA (ADM = NO)
                        User => SYSTEM (ADM = YES)
        User => SYS (ADM = NO)
        User => WKSYS (ADM = NO)
        User => SPATIAL_WFS_ADMIN_USR (ADM = NO)
        User => SPATIAL_CSW_ADMIN_USR (ADM = NO)
        Role => IMP_FULL_DATABASE (ADM = NO) which is granted to =>
                User => SYS (ADM = YES)
                User => WKSYS (ADM = NO)
                User => IMPORTER (ADM = NO)
                Role => DBA (ADM = NO) which is granted to =>
                        User => SYS (ADM = YES)
                        User => SYSMAN (ADM = NO)
                        User => AA (ADM = NO)
                        User => SYSTEM (ADM = YES)
                        Role => APPROLE (ADM = NO) which is granted t
                                User => BB (ADM = NO)
                                User => AA (ADM = NO)
                                User => SYSTEM (ADM = YES)
                Role => DATAPUMP_IMP_FULL_DATABASE (ADM = NO) which i
o =>
                        Role => DBA (ADM = NO) which is granted to =>

>

                        Us
        User => OWBSYS (AD
```

```
SQL> select name from system_privilege_map
  2  where name like '%DIRECT%';

NAME
----------------------------------------
DROP ANY DIRECTORY
CREATE ANY DIRECTORY

SQL> _
```

Check who can create or drop directories

Check who can change utl_file_dir

Check who could grant these privileges

Check who can change, create.. Procedures and libraries

Access To The Server - 10

- Securing access to the operating system is not complex but as with the data analysis there are many components, layers, hierarchy and duplication in paths
- We must understand all interfaces to the operating system
- We must understand all API's exposing these interfaces
- We must understand the privileges that allow access to the operating system
- A pattern is emerging in terms of components we must secure in Oracle

Layers, Hierarchy, Complexity

- Each of the three examples has
  - Layers of complexity
  - Multiple requirements for one area - Users
  - Multiple paths to data
  - Multiple copies of data
  - Multiple pieces of the puzzle involved with operating system objects
  - Multiple paths to the operating system
- See the pattern now?

Conclusions

- There are a few important lessons we must learn to secure data held in an Oracle database
  - We must secure the “**data**” not the software (quite obviously we MUST secure the software to achieve “**data**” security)
  - We must start with the “**data**” not the software
  - We must understand who/how/why/when “**data**” could be stolen
- Oracle security is complex though because we must consider “**where**” the “**data**” is and “**who**” can access it and “**how**”
- Often there are “**layers**” and “**duplication**”
- Careful detailed work is often needed

Any Questions?

Contact - Pete Finnigan

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

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