UKOUG Conference 2008, December 1st 2008

Oracle Security Basics

By

Pete Finnigan

Updated Monday, 24th November 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

- What is Oracle Security?
- Basic Oracle security tenets / ideas
- Why a database must be secured
- How can a database be breached?
- Key security issues
  - Discussion of problems
  - Discussion of high level fixes
- What to do next

What Is Oracle Security?

- Securely configuring an existing Oracle database?
- Designing a secure Oracle database system before implementation?
- 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!**

The Basic Tenets Of Oracle Security

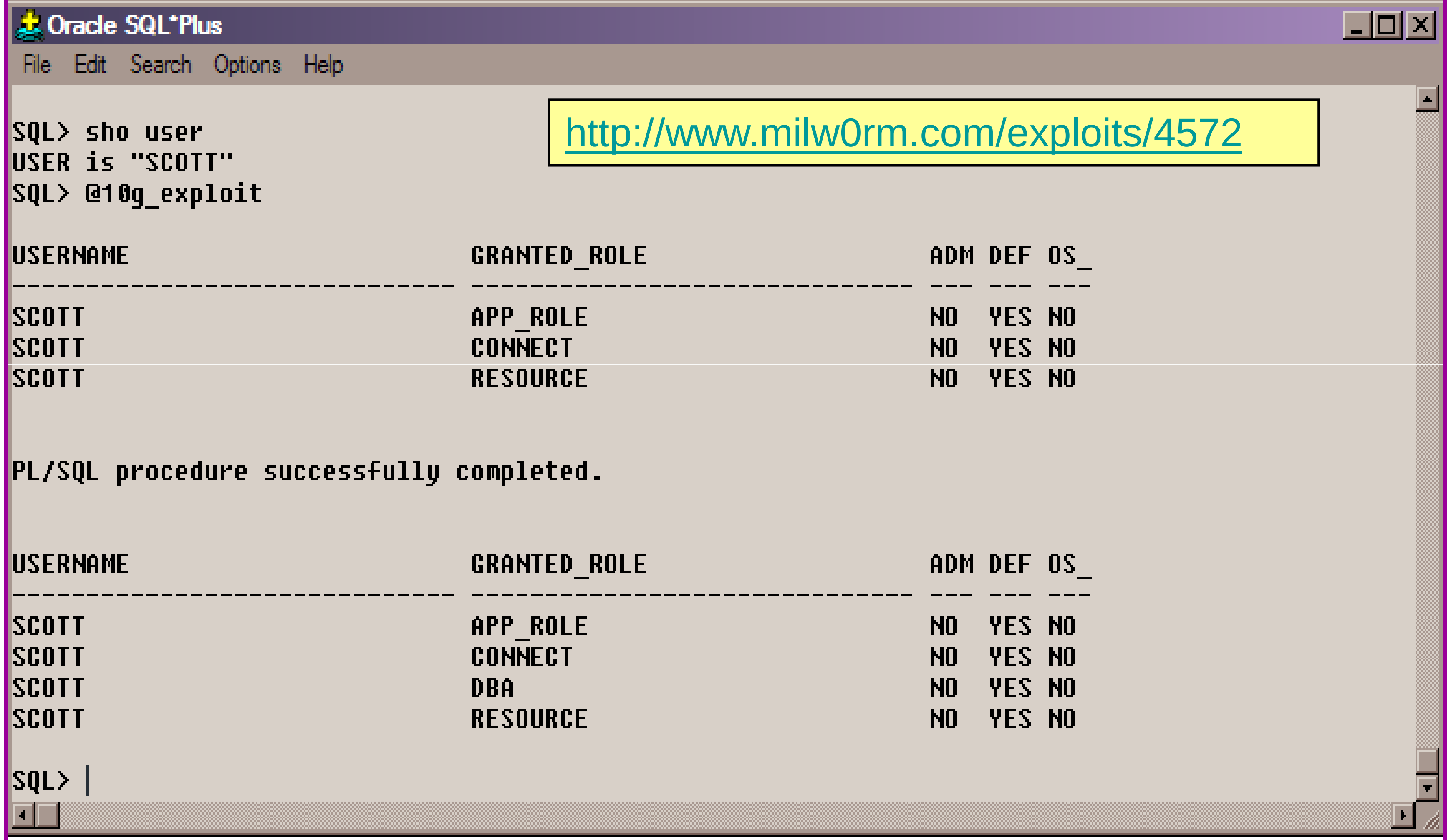
- Reduce the version / installed product to that necessary
- Reduce the users / schemas installed
- Reduce and design privileges to least privilege principal
- Lock down basic configurations
- Enable audit trails in the database
- Clean up

Reduction is the key

Why The Data Must Be Secured

- 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 traditional 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 have access to data
  - DBA’s use excessive privileges
- Data is often the target now not system access

Breaching The Database?



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> |
```

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 but concentrate on key areas and outside access

General Oracle Security Info

You need information, tools, checklists

- 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 – http://www.petefinnigan.com/tools.htm
  - Who_has scripts, CIS benchmark, Scuba, rorascanner, Metacortex, cqure, many more
- Papers, blogs, forums, books
- 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
- Websites – petefinnigan.com, cqure, RDS, Argeniss, databasesecurity.com

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

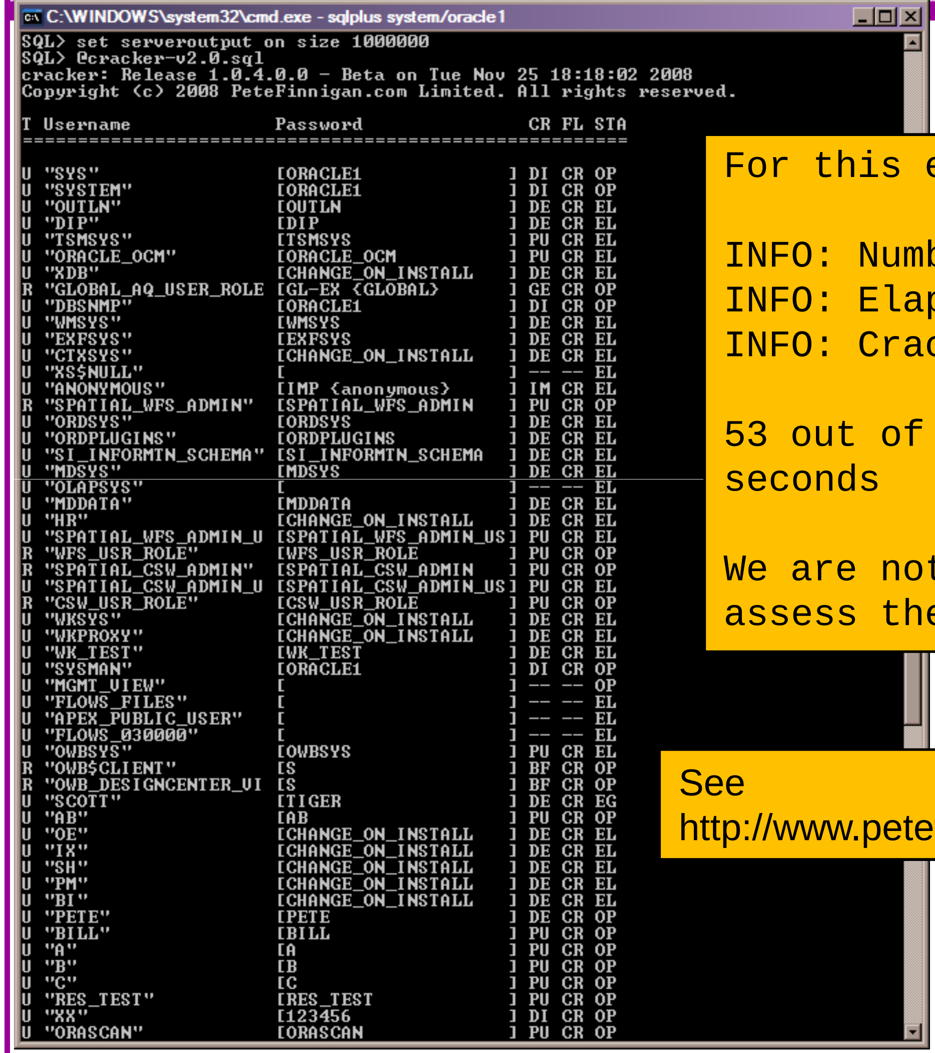
11gR1 has broken this!!

- 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
- **Do not do any of these!**

What to audit (First?)

- Perform a password audit – use a tool such as woraauthbf – http://www.soonerorlater.hu/index.khtml?article_id=513
- Reduce network access and leakage
- Review the listener
- File system
  - look for passwords
  - permissions
- Audit basic configuration
  - Parameters
  - User accounts that exist
  - Privileges on objects
  - Privileges assigned to users
- Use one of my scripts, who_can_access.sql, find_all_privs.sql, who_has_role.sql, who_has_priv.sql – see http://www.petefinnigan.com/tools.htm

Password Cracking (Easy way)



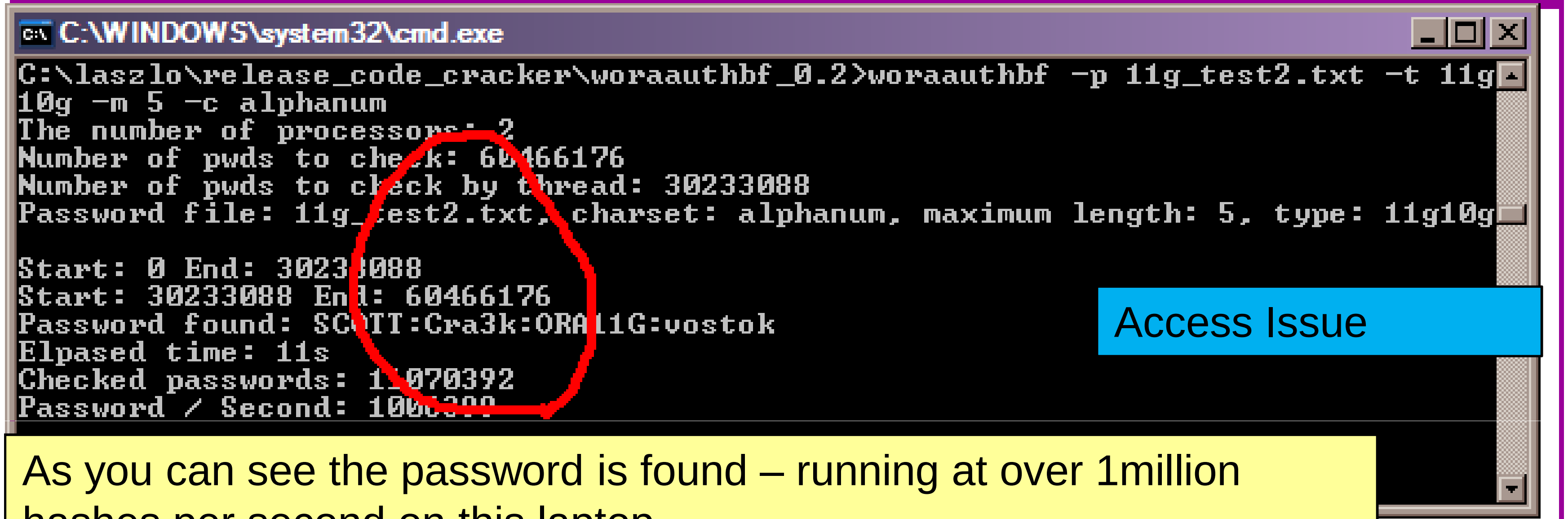
```
SQL> set serveroutput on size 1000000
SQL> @cracker-v2.0.sql
cracker: Release 1.0.4.0.0 - Beta on Tue Nov 25 18:18:02 2008
Copyright (c) 2008 PeteFinnigan.com Limited. All rights reserved.

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$NULL"            [                    ] -- -- EL
U "ANONYMOUS"          [IMP {anonymous}     ] IM CR EL
R "SPATIAL_WFS_ADMIN"  [SPATIAL_WFS_ADMIN   ] PU CR OP
U "ORDSYS"             [ORDSYS              ] DE CR EL
U "ORDPLUGINS"         [ORDPLUGINS          ] DE CR EL
U "SI_INFORMTN_SCHEMA" [SI_INFORMTN_SCHEMA  ] DE CR EL
U "MDSYS"              [MDSYS               ] DE CR EL
U "OLAPSYS"            [                    ] -- -- EL
U "MDDATA"             [MDDATA              ] DE CR EL
U "HR"                 [CHANGE_ON_INSTALL   ] DE CR EL
U "SPATIAL_WFS_ADMIN_U [SPATIAL_WFS_ADMIN_US] PU CR EL
R "WFS_USR_ROLE"       [WFS_USR_ROLE        ] PU CR OP
R "SPATIAL_CSW_ADMIN"  [SPATIAL_CSW_ADMIN   ] PU CR OP
U "SPATIAL_CSW_ADMIN_U [SPATIAL_CSW_ADMIN_US] PU CR EL
R "CSW_USR_ROLE"       [CSW_USR_ROLE        ] PU CR OP
U "WKSYS"              [CHANGE_ON_INSTALL   ] DE CR EL
U "WKPROXY"            [CHANGE_ON_INSTALL   ] DE CR EL
U "WK_TEST"            [WK_TEST             ] DE CR EL
U "SYSMAN"             [ORACLE1             ] DI CR OP
U "MGMT_VIEW"          [                    ] -- -- OP
U "FLOWS_FILES"        [                    ] -- -- EL
U "APEX_PUBLIC_USER"   [                    ] -- -- EL
U "FLOWS_030000"       [                    ] -- -- EL
U "OWBSYS"             [OWBSYS              ] PU CR EL
R "OWB$CLIENT"         [S                   ] BF CR OP
R "OWB_DESIGNCENTER_VI [S                   ] BF CR OP
U "SCOTT"              [TIGER               ] DE CR EG
U "AB"                 [AB                  ] PU CR OP
U "OE"                 [CHANGE_ON_INSTALL   ] DE CR EL
U "IX"                 [CHANGE_ON_INSTALL   ] DE CR EL
U "SH"                 [CHANGE_ON_INSTALL   ] DE CR EL
U "PM"                 [CHANGE_ON_INSTALL   ] DE CR EL
U "BI"                 [CHANGE_ON_INSTALL   ] DE CR EL
U "PETE"               [PETE                ] DE CR OP
U "BILL"               [BILL                ] PU CR OP
U "A"                  [A                   ] PU CR OP
U "B"                  [B                   ] PU CR OP
U "C"                  [C                   ] PU CR OP
U "RES_TEST"           [RES_TEST            ] PU CR OP
U "XX"                 [123456              ] DI CR OP
U "ORASCAN"            [ORASCAN             ] PU CR OP
```

```
For this example run

INFO: Number of crack attempts = [61791]
INFO: Elapsed time = [4.36 Seconds]
INFO: Cracks per second = [14170]

53 out of 60 accounts cracked in 4.3
seconds

We are not trying to break in BUT trying to
assess the “real security level”
```

See http://www.petefinnigan.com/oracle_password_cracker.htm

Access Issue

Password Cracker (Hard Way)



```
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
```

Access Issue

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

Woraauthbf can also be used to crack from authentication sessions

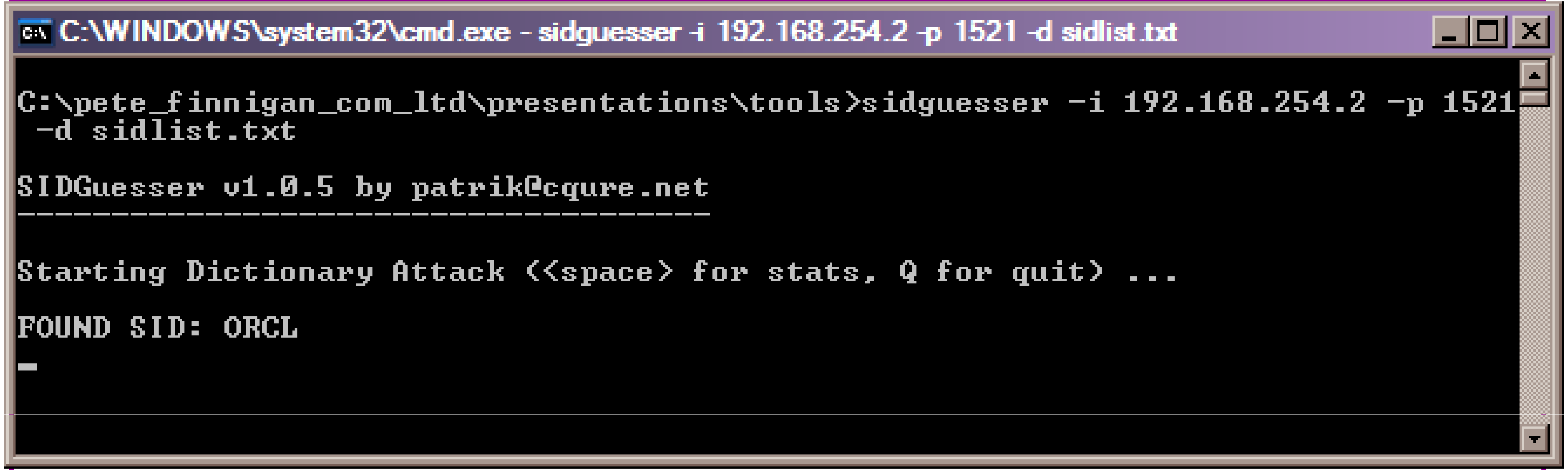
Woraauthbf can be used in dictionary or brute force mode

Use it to supplement the PL/SQL based cracker

http://www.soonerorlater.hu/download/woraauthbf_src_0.22.zip

http://www.soonerorlater.hu/download/woraauthbf_0.22.zip

SIDGuesser


C:\WINDOWS\system32\cmd.exe - sidguesser -i 192.168.254.2 -p 1521 -d sidlist.txt

```
C:\pete_finnigan_com_ltd\presentations\tools>sidguesser -i 192.168.254.2 -p 1521
 -d sidlist.txt

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

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

FOUND SID: ORCL
_
```

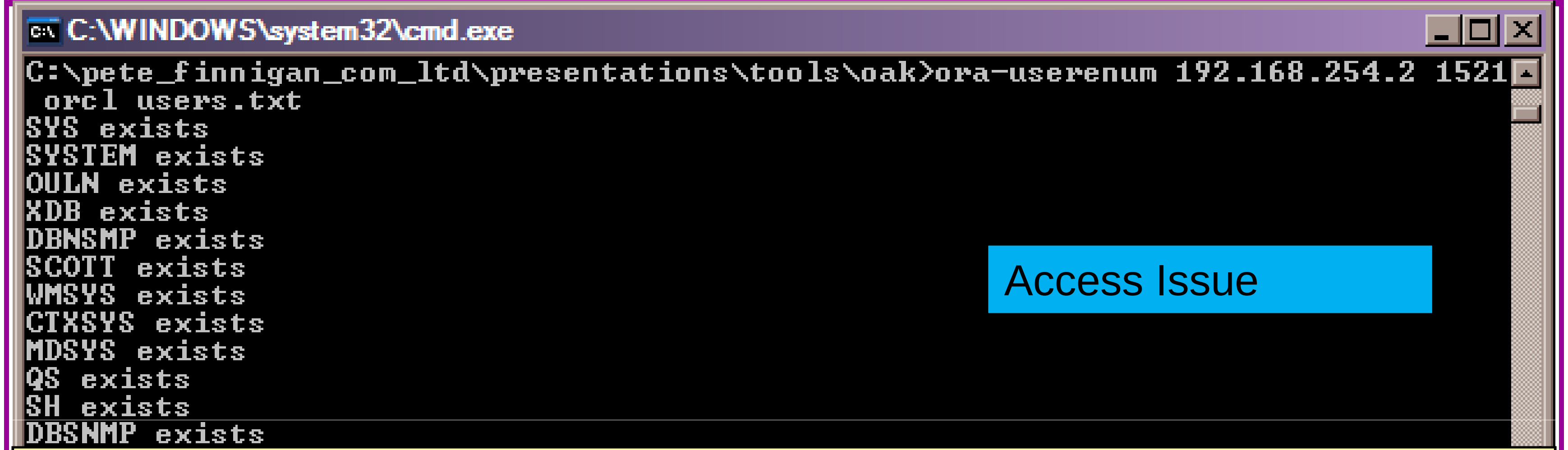
From http://www.cqure.net/tools/SIDGuesser_win32_1_0_5.zip

This is not an audit tool BUT you should understand what it does

A better approach is to use the dictionary list in a text editor and check if your service name/SID is listed

Access Issue

User Enumeration



```
C:\pete_finnigan_com_ltd\presentations\tools\oak>ora-userenum 192.168.254.2 1521
 orcl 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
```

Access Issue

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

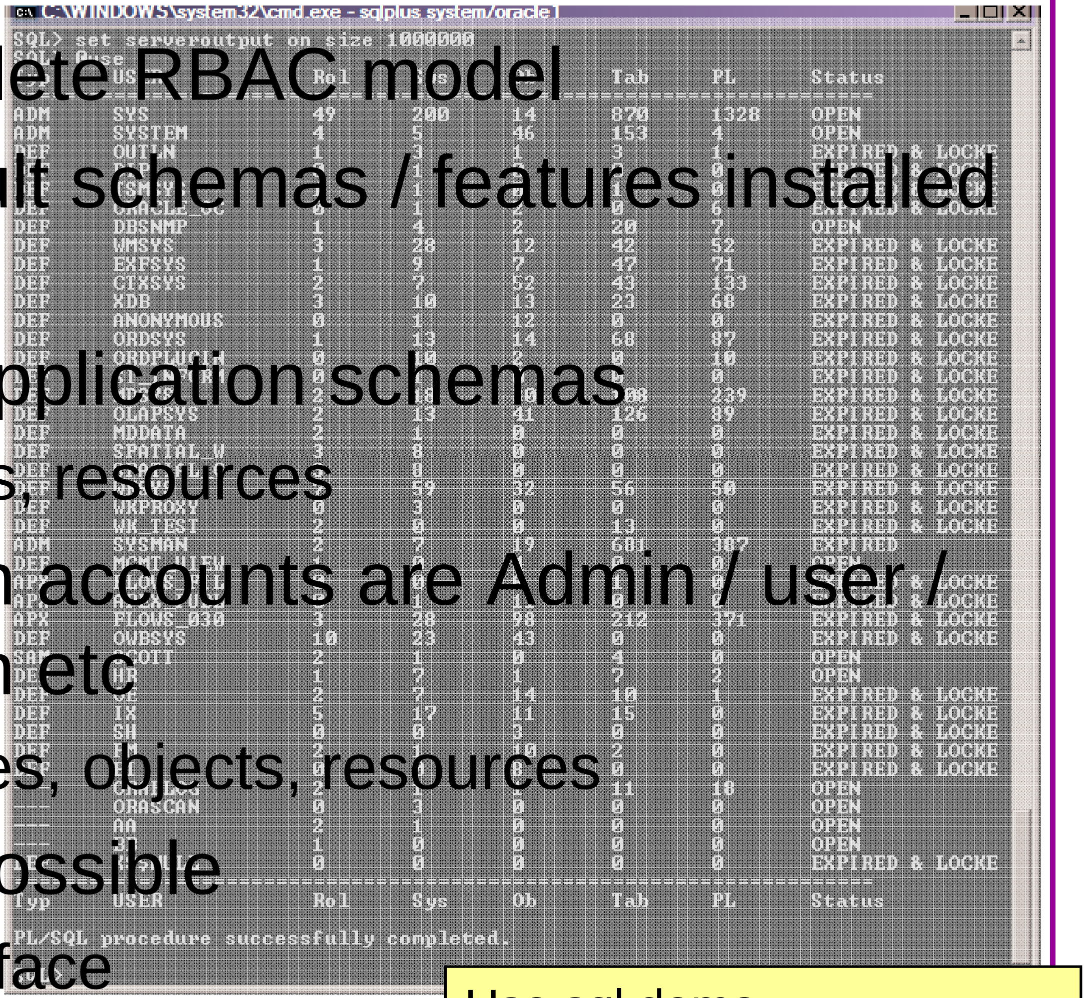
SYS and SYSTEM always exist so passwords guesses can be attempted

Other users can “almost” certainly be there as well – DBSNMP / OUTLN for instance

This is not an audit tool; for an audit reduce the number of default schemas

RBAC

- Review the complete RBAC model
- Understand default schemas / features 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
  - – reduce attack surface



```
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         [illegible] 0       0         EXPIRED & LOCKE
DEF       TSMSYS       [illegible] 1       [illegible] 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         [illegible] [illegible] [illegible] 0   EXPIRED & LOCKE
DEF       MDSYS        2         18        [illegible] [illegible] 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       [illegible]  [illegible] 8       0         0         0         EXPIRED & LOCKE
DEF       [illegible]  [illegible] 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    [illegible] 0       [illegible] 0       0         OPEN
APX       FLOWS_FIL    [illegible] 0       [illegible] 1       0         EXPIRED & LOCKE
APX       APEX_PUBL    [illegible] 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       [illegible]  [illegible] [illegible] [illegible] 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
DEF       XS$NULL      0         0         0         0         0         EXPIRED & LOCKE
=================================================================================
Typ       USER         Rol       Sys       Ob        Tab       PL        Status

PL/SQL procedure successfully completed.

SQL>
```

Use.sql demo

Secure Listener by Default?

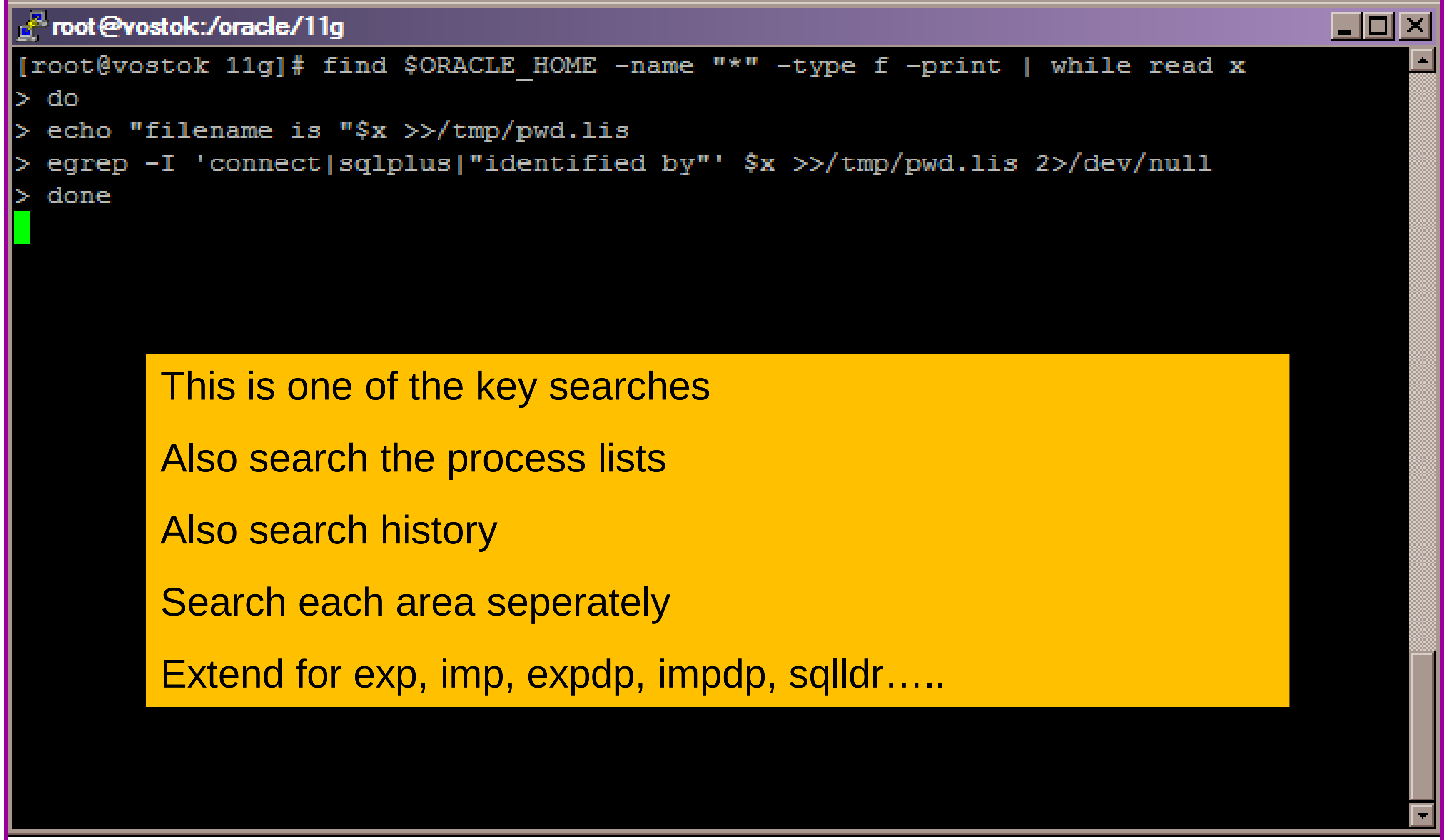
```
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 11.1.0.6.0 -
   Production
Start Date                31-OCT-2007 09:06:14
Uptime                    0 days 4 hr. 56 min. 27 sec
Trace Level               off
Security                  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 i
  Instance "ORA11G", sta
Service "ORA11GXDB" has
  Instance "ORA11G", sta
Service "ORA11G_XPT" has
  Instance "ORA11G", sta
```

Turn on admin restrictions

Ensure no password in >10g

Use valid node checking / Firewall – {Access Issue}

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

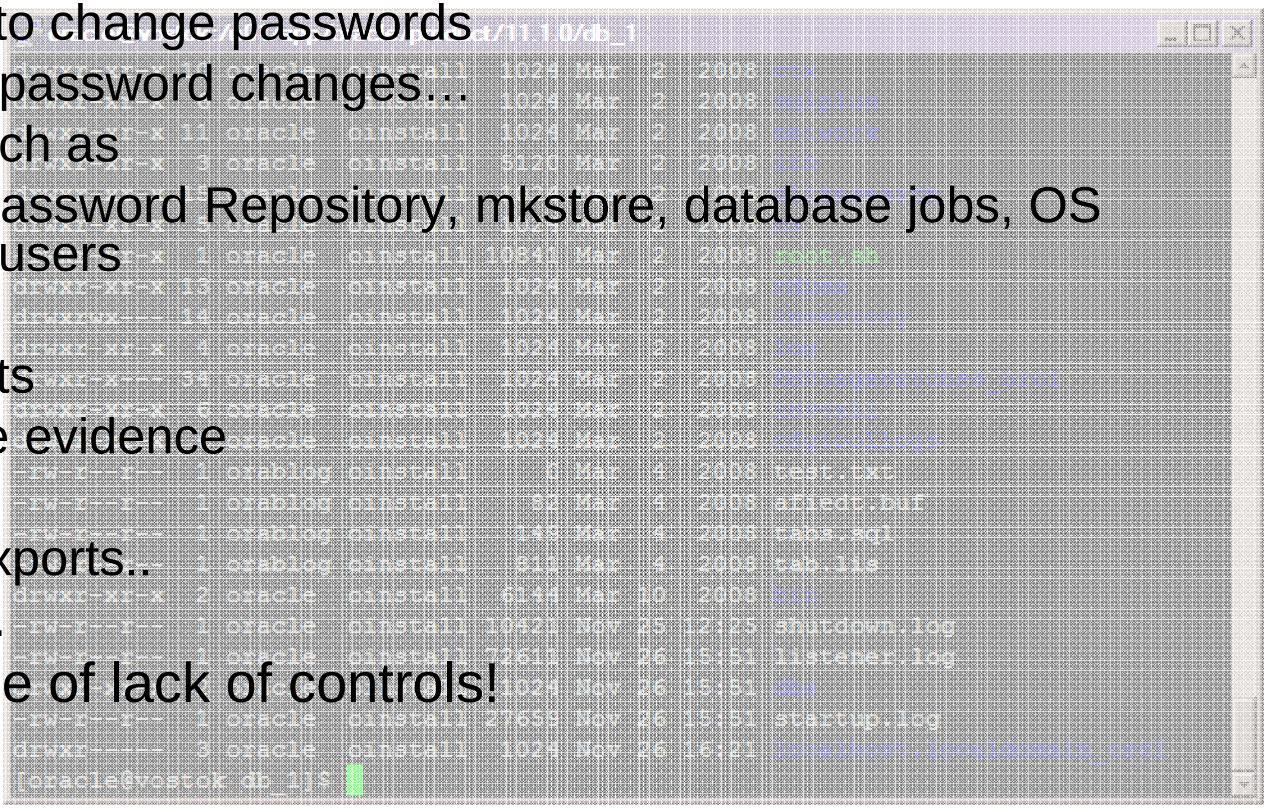
Also search history

Search each area seperately

Extend for exp, imp, expdp, impdp, sqlldr…..

Clean Up

- This is the security killer in most systems I see
- Often file systems include
  - Scripts with passwords or
  - worse rules to change passwords
  - Evidence of password changes…
  - Use tools such as
    - Oracle Password Repository, mkstore, database jobs, OS external users
- Clean up
  - ad-hoc scripts
  - Maintenance evidence
  - Trace files
  - Data files, exports..
  - Audit logs….
- All are evidence of lack of controls!



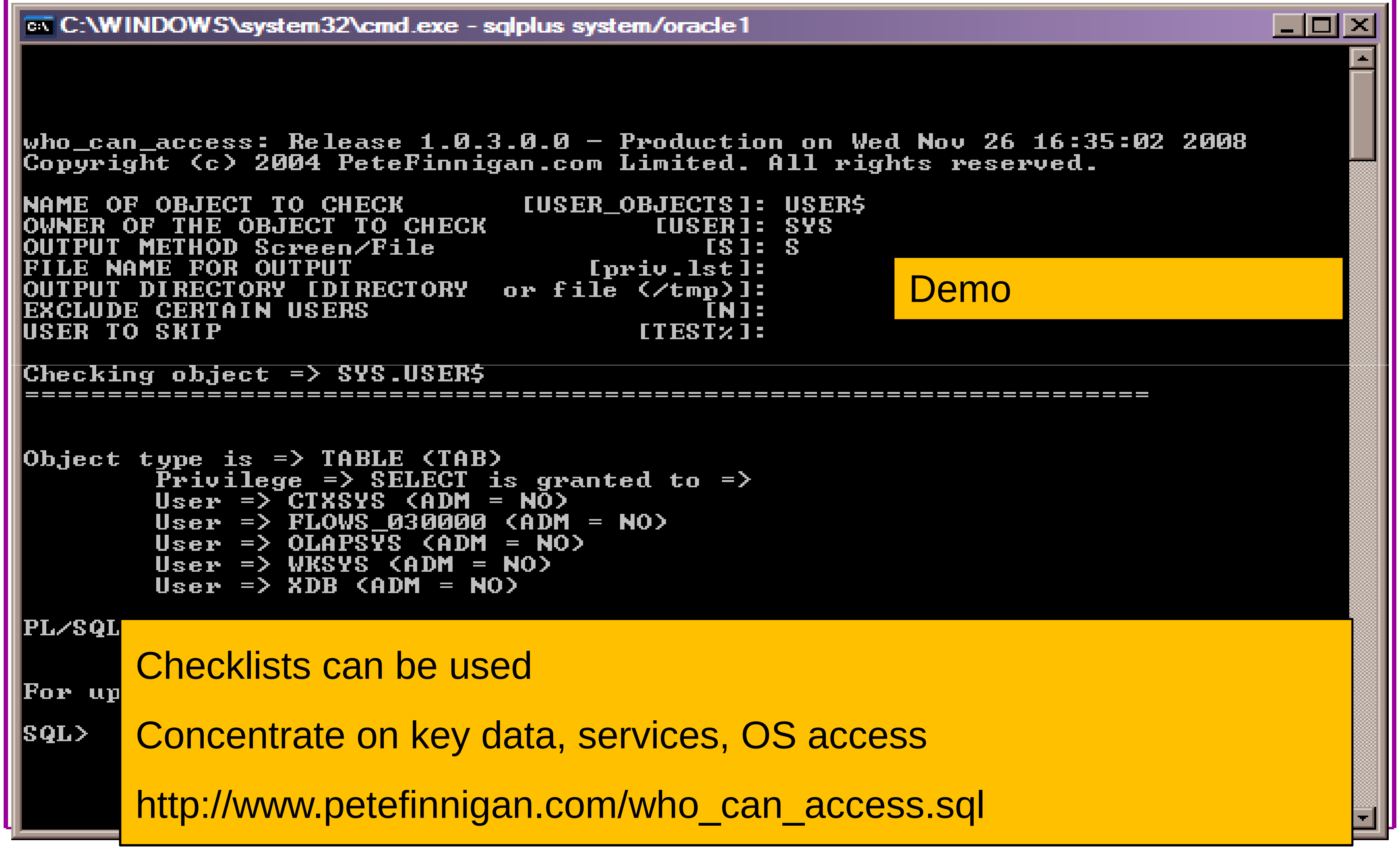
[illegible]/11.1.0/db_1

```
[illegible] oracle  oinstall  1024 Mar  2  2008 ctx
[illegible] oracle  oinstall  1024 Mar  2  2008 sqlplus
drwxr-xr-x 11 oracle  oinstall  1024 Mar  2  2008 network
drwxr-xr-x  3 oracle  oinstall  5120 Mar  2  2008 lib
[illegible]
drwxr-xr-x  5 oracle  oinstall  1024 Mar  2  2008 [illegible]
-rwxr-xr-x  1 oracle  oinstall 10841 Mar  2  2008 root.sh
drwxr-xr-x 13 oracle  oinstall  1024 Mar  2  2008 rdbms
drwxrwx--- 14 oracle  oinstall  1024 Mar  2  2008 inventory
drwxr-xr-x  4 oracle  oinstall  1024 Mar  2  2008 log
drwxr-x--- 34 oracle  oinstall  1024 Mar  2  2008 EMStagePatches_orcl
drwxr-xr-x  6 oracle  oinstall  1024 Mar  2  2008 install
[illegible] oracle  oinstall  1024 Mar  2  2008 cfgtoollogs
-rw-r--r--  1 orablog oinstall     0 Mar  4  2008 test.txt
-rw-r--r--  1 orablog oinstall    82 Mar  4  2008 afiedt.buf
-rw-r--r--  1 orablog oinstall   149 Mar  4  2008 tabs.sql
-rw-r--r--  1 orablog oinstall   811 Mar  4  2008 tab.lis
drwxr-xr-x  2 oracle  oinstall  6144 Mar 10  2008 bin
-rw-r--r--  1 oracle  oinstall 10421 Nov 25 12:25 shutdown.log
-rw-r--r--  1 oracle  oinstall 72611 Nov 26 15:51 listener.log
[illegible]  1024 Nov 26 15:51 dbs
-rw-r--r--  1 oracle  oinstall 27659 Nov 26 15:51 startup.log
drwxr-----  3 oracle  oinstall  1024 Nov 26 16:21 localhost.localdomain_orcl
[oracle@vostok db_1]$
```

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
  - Do not use default accounts
  - Do not use default roles including DBA
  - Do not use default passwords

Access To Key Data (SYS.USER$)



```
who_can_access: Release 1.0.3.0.0 - Production on Wed Nov 26 16:35:02 2008
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK       [USER_OBJECTS]: USER$
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.USER$
====================================================================


Object type is => TABLE (TAB)
        Privilege => SELECT is granted to =>
        User => CTXSYS (ADM = NO)
        User => FLOWS_030000 (ADM = NO)
        User => OLAPSYS (ADM = NO)
        User => WKSYS (ADM = NO)
        User => XDB (ADM = NO)

PL/SQL

For up

SQL>
```

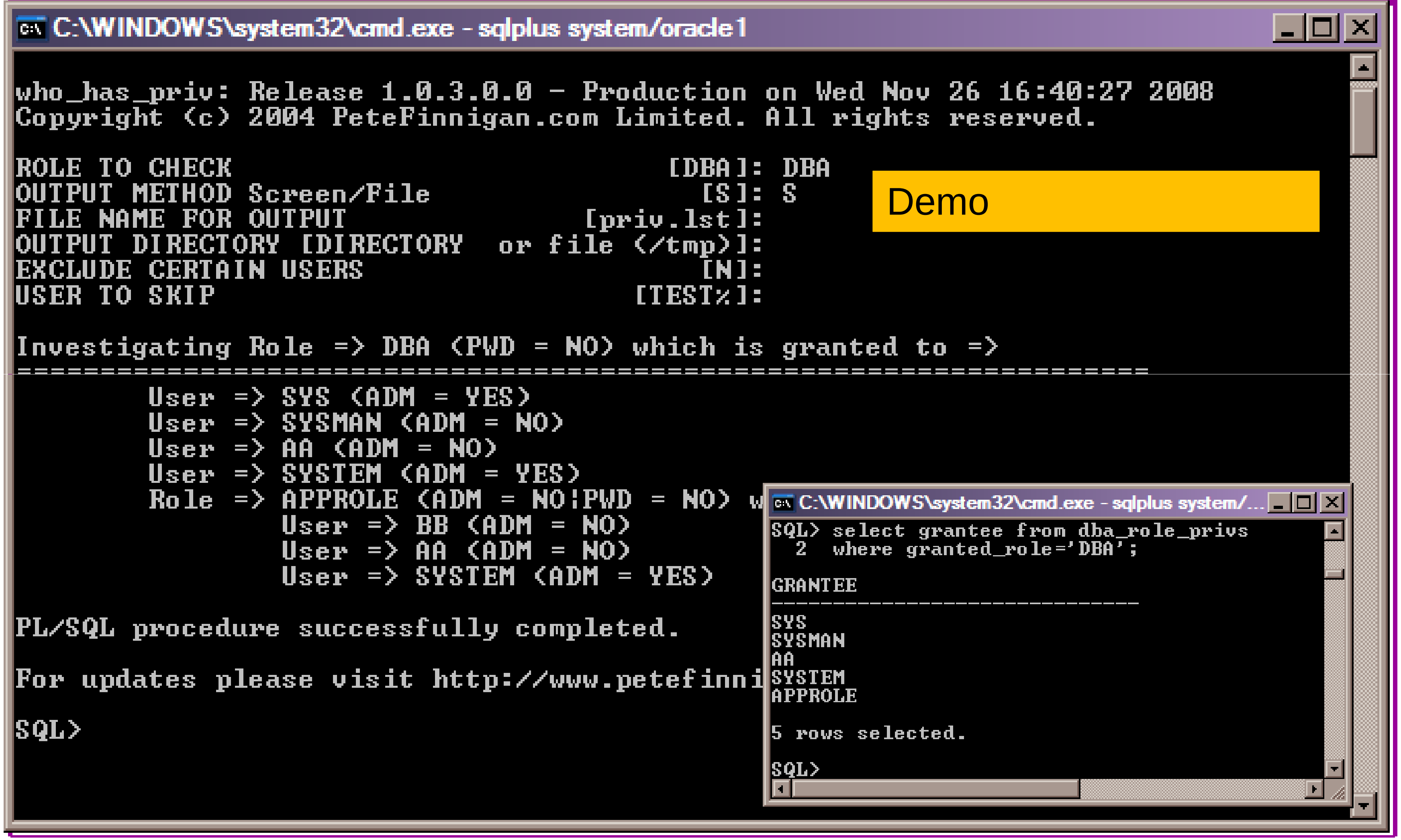
Demo

Checklists can be used

Concentrate on key data, services, OS access

http://www.petefinnigan.com/who_can_access.sql

Who Has Key Roles

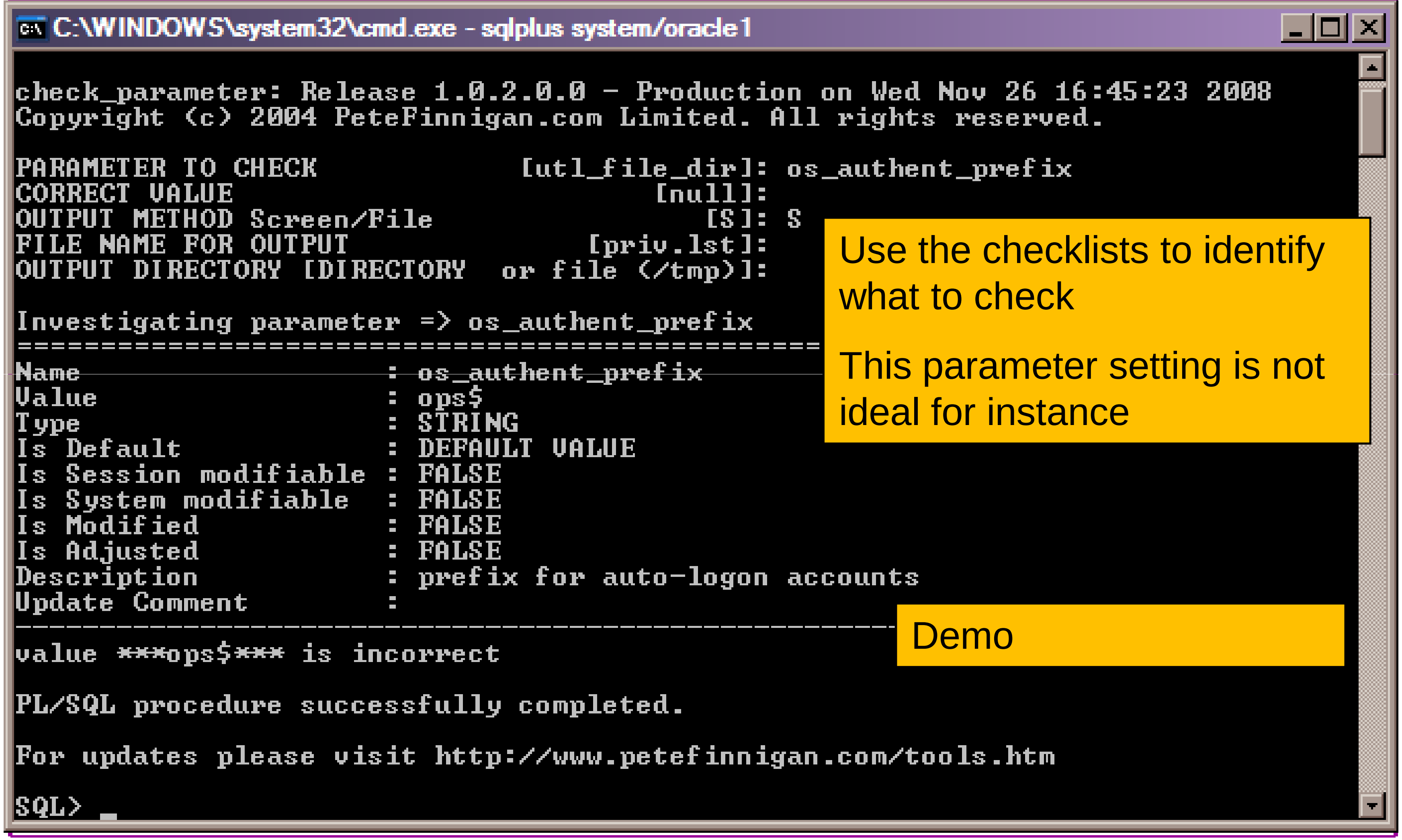


```
who_has_priv: Release 1.0.3.0.0 - Production on Wed Nov 26 16:40:27 2008
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

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 => AA (ADM = NO)
        User => SYSTEM (ADM = YES)
        Role => APPROLE (ADM = NO|PWD = NO) w
                User => BB (ADM = NO)
                User => AA (ADM = NO)
                User => SYSTEM (ADM = YES)

PL/SQL procedure successfully completed.

For updates please visit http://www.petefinni

SQL>
```

Demo

```
SQL> select grantee from dba_role_privs
  2  where granted_role='DBA';

GRANTEE
------------------------------

SYS
SYSMAN
AA
SYSTEM
APPROLE

5 rows selected.

SQL>
```

Check Parameters



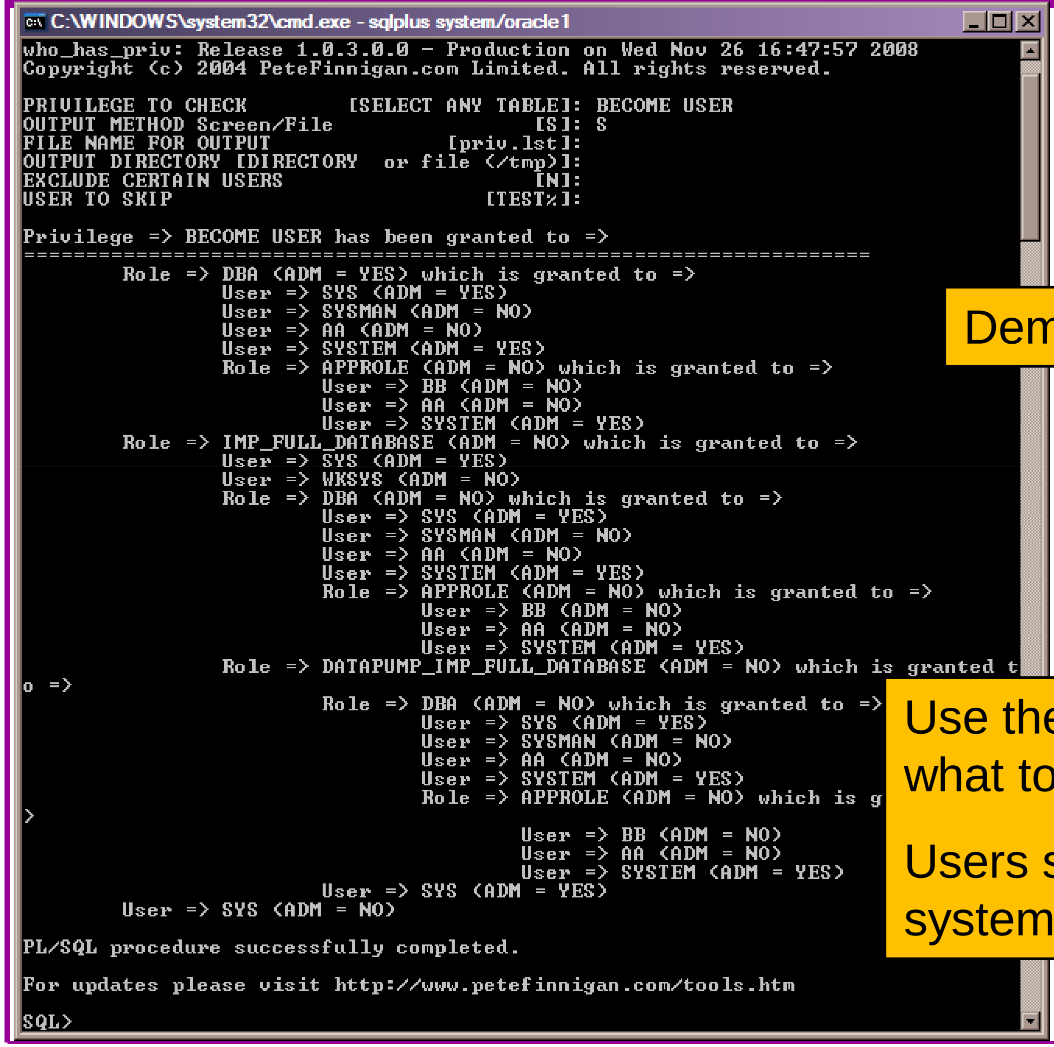
```
check_parameter: Release 1.0.2.0.0 - Production on Wed Nov 26 16:45:23 2008
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

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

Check System Privileges



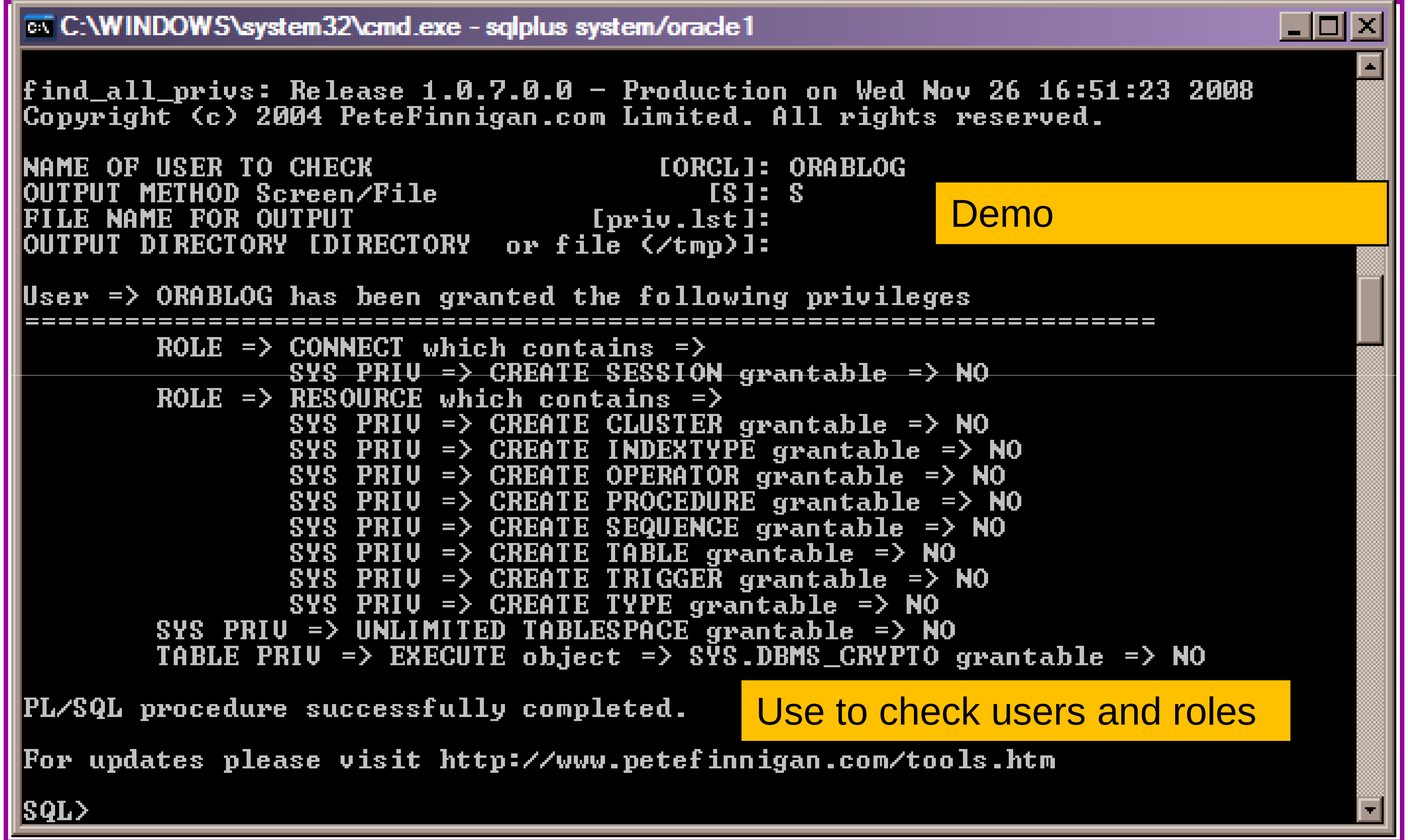
```
who_has_priv: Release 1.0.3.0.0 - Production on Wed Nov 26 16:47:57 2008
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

PRIVILEGE TO CHECK        [SELECT ANY TABLE]: BECOME USER
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%]:

Privilege => BECOME USER 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)
        Role => IMP_FULL_DATABASE (ADM = NO) which is granted to =>
                User => SYS (ADM = YES)
                User => WKSYS (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 to =>
                                User => BB (ADM = NO)
                                User => AA (ADM = NO)
                                User => SYSTEM (ADM = YES)
                Role => DATAPUMP_IMP_FULL_DATABASE (ADM = NO) which is granted t
o =>
                        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 g
>

                                        User => BB (ADM = NO)
                                        User => AA (ADM = NO)
                                        User => SYSTEM (ADM = YES)
                        User => SYS (ADM = YES)
        User => SYS (ADM = NO)

PL/SQL procedure successfully completed.

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

SQL>
```

Demo

Use the checklists to identify what to check

Users should not have system privileges

Who Has What Privileges

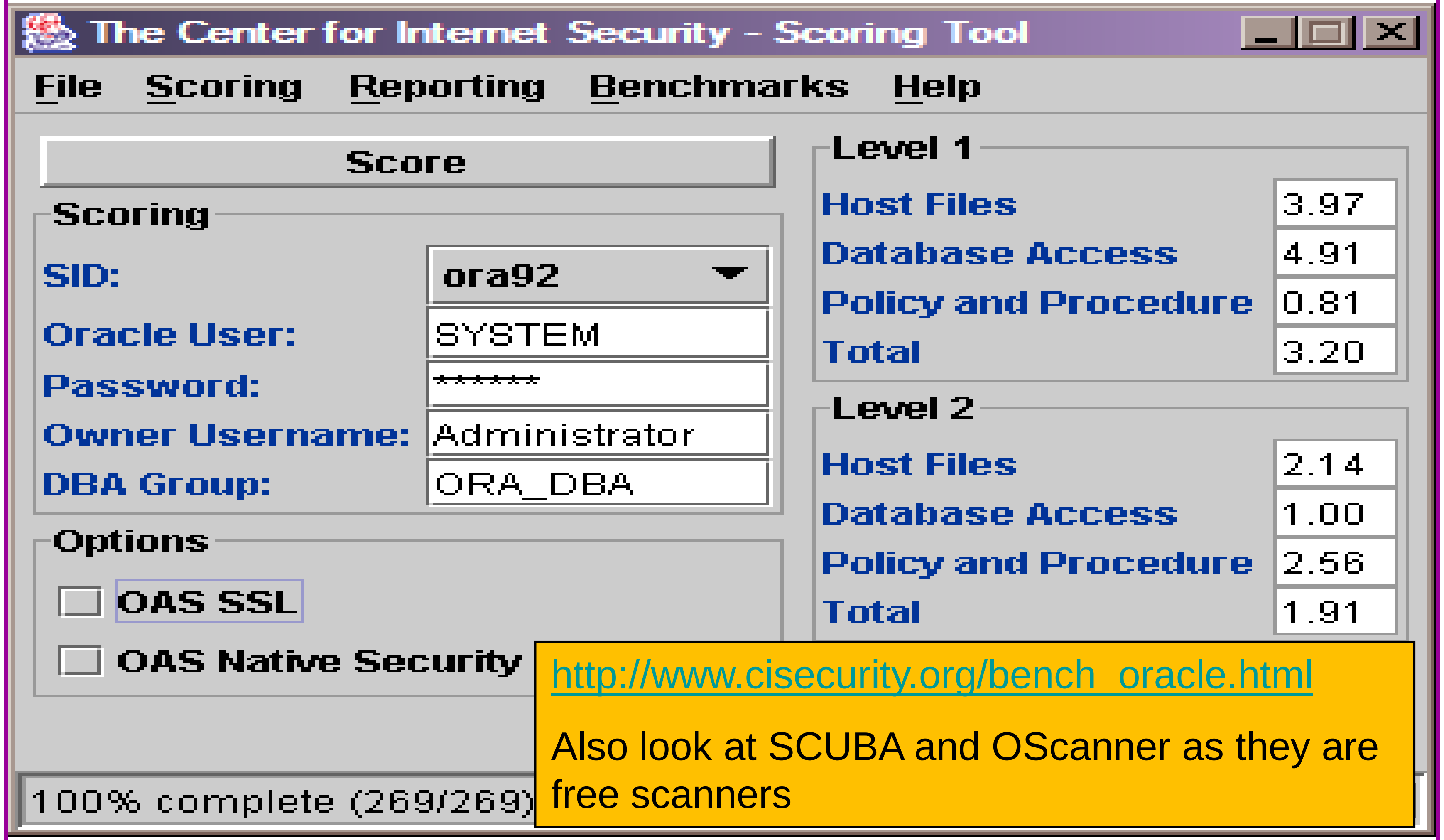


```
find_all_privs: Release 1.0.7.0.0 - Production on Wed Nov 26 16:51:23 2008
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

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

User => ORABLOG has been granted the following privileges
====================================================================
        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
        TABLE PRIV => EXECUTE object => SYS.DBMS_CRYPTO grantable => NO

PL/SQL procedure successfully completed.

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

SQL>
```

Demo

Use to check users and roles

CIS Benchmark


The Center for Internet Security - Scoring Tool
File Scoring Reporting Benchmarks Help
Score

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

100% complete (269/269)

http://www.cisecurity.org/bench_oracle.html

Also look at SCUBA and OScanner as they are free scanners

Get The Basics Right

- OK, we have covered a lot of information
- Concentrate on
  - Checking and strengthening users passwords
  - Removing default schemas and software not needed
  - Reduce leakage of critical data (passwords and more) from the database and filesystems

Get The Basics Right (2)

- Don’t leak network data to allow connection attempts
- Use firewalls or valid node checking to protect the database [Stop direct connections]
- Review privileges and access to key data
- Confirm key configuration is set securely

What To Do Next

- Fix the basics, then what?
- Use the project lockdown or one of the good checklists to do a more detailed review
- Ensure sound audit plan is in place
- Understand how hackers may steal your data
- This way **YOU** can understand how to protect it
- Monitor the database security for compliance

Audit The Oracle Database

- Operating security Checklists
  - CIS benchmarks for Windows, Linux, Solaris and more
  - OS check tools – The CIS benchmarks are useful – others are available
- Oracle security checks
  - Most tools are windows centric – don't install them on the prod database servers if you run Windows
  - Audit by hand to gain understanding
  - Audit using a free or commercial tool
  - Get professional help
- Oracle security checklists
  - use and work through
  - these are great resources to start with

Use the tools we have shown

Get the basics right first

Perform Hardening

- Reduce the features and functions installed – OS and DB
- Harden the operating system
- Review RBAC for all users
- Remove defaults – settings, users, passwords
- Decide on secure configuration settings
- Clean up
- 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

Create A Monitoring Process

- Once you are secure or on the way to being secure
- Realise its not a “one-off” process
- Constant monitoring of the database is necessary because
  - New issues arise
  - The database can change shape
  - Your knowledge increases
- Create a monitoring process – this can be a policy, a set of scripts, a commercial tool

Conclusions

- We didn’t mention CPU’s – Apply them – they are only part of the process
- Think like a hacker
- Get the basics right first – stop attempted connections or cracking
- Sort out the RBAC, configuration, installed software and privileges
- Get the basics right first

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