

UKOUG Conference, December 7th 2007

Oracle Security Tools

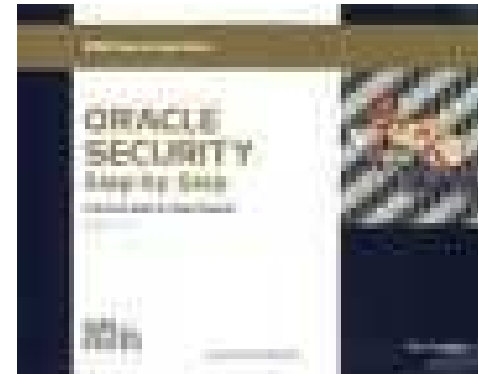
By

Pete Finnigan

Written Friday, 19th October 2007

Introduction - Commercial Slide. ☹️

- PeteFinnigan.com Limited
- Founded February 2003
- CEO Pete Finnigan
- Clients UK, States, Europe
- Specialists in researching and securing Oracle databases
- <http://www.petefinnigan.com>
- Consultancy and training available
- Author of Oracle security step-by-step
- Published many papers, regular speaker (UK, USA)



Agenda

- Where to find Oracle security tools
- Look at the types of tools (categorize)
- Consider free and commercial tools
- Protecting against Oracle Security tools
- A quick look at what Oracle provides
- Demo and summarise some of the key tools that can be used

Where To Find Oracle Security Tools

Pete Finnigan - Oracle and Oracle security information - Microsoft Internet Explorer

Address: <http://www.petefinnigan.com/tools.htm>

Pete Finnigan is the author of the SANS book Oracle security step-by-step - a survival guide for Oracle security. Pete also has written many papers about Oracle security. [petefinnigan.com](http://www.petefinnigan.com) is the place for free Oracle security information, white papers, links to other resources, free scripts tools and products and professional Oracle security audit services.

For over 100 Oracle security white papers see [here](#).

PeteFinnigan.com Tools

All of the scripts and tools provided here are available free. You can do anything you want with them commercial or non commercial as long as the copyrights and this notice are not removed or edited in any way. The scripts cannot be posted / published / hosted or whatever anywhere else except at www.petefinnigan.com.

Although every care has been taken to ensure that they do not cause any damage caused by their use.

This page includes scripts written by Pete Finnigan.com and also links to useful Oracle security based tools written by others. The first section are Pete Finnigan's Tools.

Tool	By	Description
find_all_privs.sql	pete@petefinnigan.com	This short script can be used to find all of the privileges granted to a particular user. It includes Roles, system privileges and object privileges. If a role is encountered then it recursively looks for the roles, system privileges and object privileges granted to the roles and so on..... The output can be directed to either the 'Screen or to a 'File'. This is prompted for at run time. If a 'File is chosen then a file name and output directory are needed. If 'File is chosen then the directory used needs to be enabled via utl_file_dir prior to 9iR2 and with a directory object after that.
who_has_role.sql	pete@petefinnigan.com	This short script is the second in a series of four scripts to

Oracle Security Tool Categories

- Discovery tools
 - User enumeration – OAK toolkit
 - Sid guessing – RDS, Cqure, THC
 - Connect brute force – bfora.pl
 - SYSDBA brute force – Paul Wright
 - Listener enumerators – nmap, metacortex, tnsprobe, WinSID
- Testing tools
 - Password crackers – orabf, woraauthbf, checkpwd
 - Listener enumeration – integrigy, DokFleed, tnscommand
 - Default passwords – PeteFinnigan.com
 - Inguma – Joxean Koret
 - Backtrack CD

Oracle Security Tool Categories (2)

- Scanners
 - Listener scanners – Integrity, DokFleed
 - CIS Benchmark – old but the best free scanner
 - Scuba - Imperva
 - RoraScanner – Rory McCune
 - Audit scripts (who_has_priv) – Pete Finnigan
 - Commercial – AppDetective, Squirrel, AuditPro
- Fuzzers – Joxean Koret script + inguma
- Hardening scripts (similar to SQLsecurity.com for SQL Server) – none that I know of

Oracle Security Tool Categories (3)

- Audit Trail software
 - many e.g. SQL Guard from Guardium
 - No free solutions in same space
 - Many built in solutions
- Database IDS / IPS
 - Many e.g Hedgehog from Sentrigo
 - No free solutions in same space
- In-line Patching – BlueLane patchpoint and virtualshield
- Encryption
 - small number of players including Application Security Inc
 - Some free software but no GUI solutions

Free And Commercial

Area	Free	Commercial
Discovery	X	X
Testing	X	X
Scanner	X	X
Fuzzing	X	
Hardening		
Audit Trail		X
IDS / IPS / Patching		X
Encryption		X

This is not scientific but a simple look at the spread of tools between commercial and free - a trend is visible

Does Oracle Provide Anything?

- None of the tools listed above are supplied by Oracle as complete tools BUT
 - Oracle supplies a default password tool
 - 11gR1 has a default password check built in
 - There are no Oracle scanners (at least not public)
 - Oracle does provide various audit scripts (quite old) on Metalink
 - Oracle includes many built in audit solutions and audit vault
 - Oracle also provides many encryption solutions

Support And Maintenance

- All Commercial products can include – support and upgrade
- Free tools – depends on developers and
 - Is this an issue?
 - We have source code in lots of cases
 - A lot of tools can be extended
 - A problem of research?
 - A problem of wasted (duplicate) efforts
 - Commercial / free requires careful considerations

Supporting Role Tools

- Whilst we are talking about Oracle security tools we should not ignore the platform and network
 - This should include database discovery using network security tools such as nmap, amap, nessus
 - This should also include platform checks. The CIS benchmark tools are very good as a start in this area

Security Issues With Tools

- Protect against tools run on your own databases
- Just as you can use for audit / testing etc these tools can also be used against you
- Beware some *rare* tools have virus code included to allow the author to take over your machine
- One legitimate tool is recognised as a virus / worm
- Choose extendable tools with source, then from trusted sources.
- Protection methods? – many and varied

Some Demonstrations

- Sidguess – Patrik Karlsson
- User Enumeration – OAK – David Litchfield
- Default passwords – 11g plus Pete Finnigan list
- Password cracker – woraaauthbf
- SYSDBA brute force – Paul Wright
- Listener checks - Integrity
- Scanners
 - Scuba - imperva
 - CIS benchmark
 - OScanner
- Privilege checks – PeteFinnigan.com scripts

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) ...

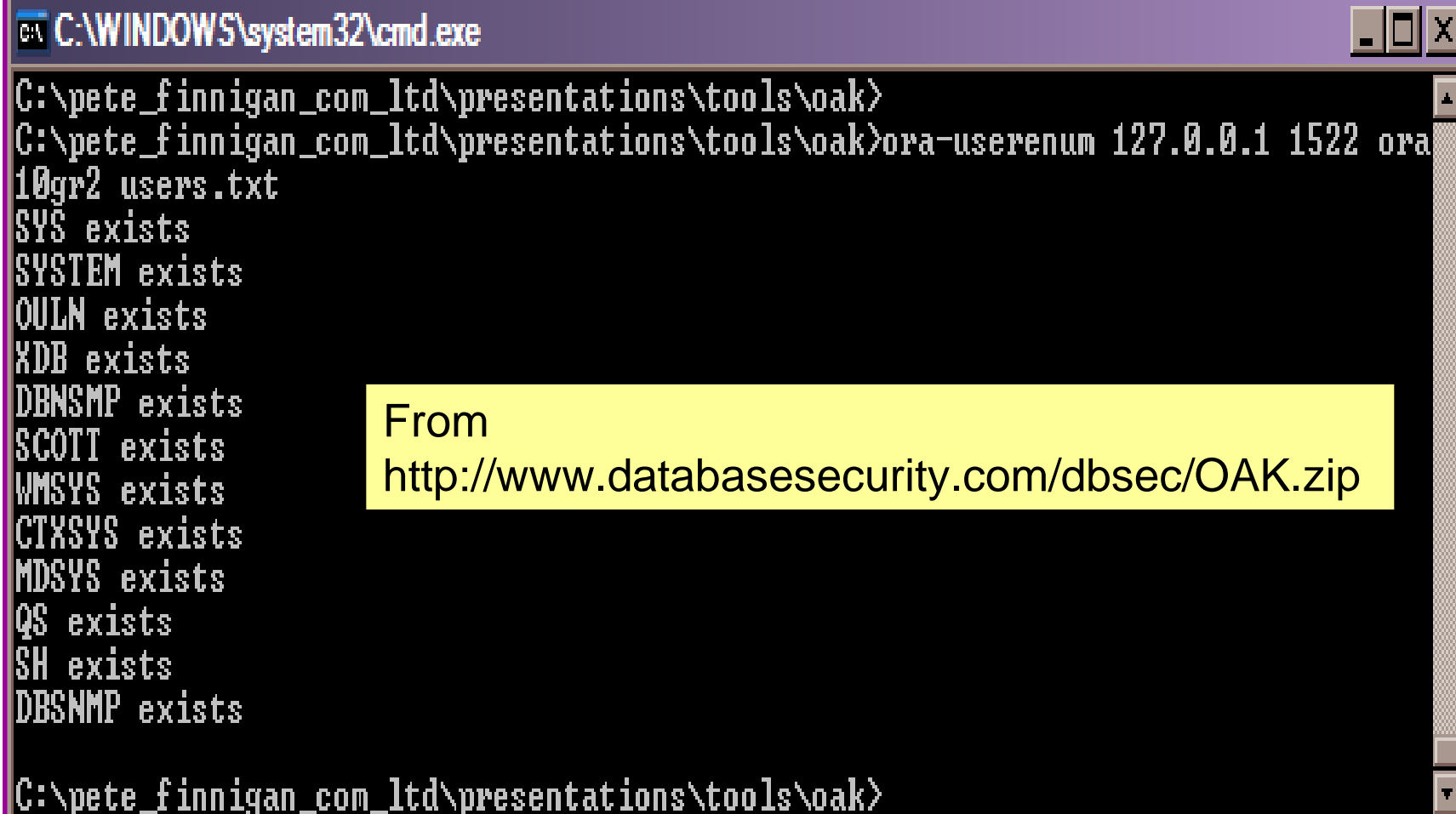
C:\pete_finnigan_com_ltd\presentations\tools>sidguesser -i 127.0.0.1 -p 1522 -d
sidlist.txt

SIDGuesser v1.0.5 by patrik@cqure.net
-----
Starting Dictionary Attack <<space> for stats, Q for quit) ...

FOUND SID: ORA10GR2

C:\pete_finnigan_com_ltd\presentations\tools>
From http://www.cqure.net/tools/SIDGuesser_win32_1_0_5.zip
```

User Enumeration



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

Default Password Check

```
SQL> select * from dba_users_with_defpwd;
```

```
USERNAME
```

```
-----
```

```
DIP
```

```
MDSYS
```

```
WK_TEST
```

```
CTXSYS
```

```
OUTLN
```

```
EXFSYS
```

```
MDDATA
```

```
ORDPLUGINS
```

```
ORDSYS
```

```
XDB
```

```
SI_INFORMTN_SCHEMA
```

```
WMSYS
```

```
12 rows selected.
```

Alternative is to use woraauthbf with a default file

See

http://www.petefinnigan.com/default/default_password_list.htm

11g Uses the old 10gR2 hash

No passwords available

690 records in the table

Remember if found you would still need to resolve the case sensitive password in 11g if its not all one case

Can implement your own version of the same

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:\WINDOWS\system32\cmd.exe
C:\laszlo\release_code_cracker\woraauthbf_0.2>woraauthbf -p 11g_test2.txt -t 11g
10g -m 5 -c alphanum
The number of processors: 2
Number of pwds to check: 60466176
Number of pwds to check by thread: 30233088
Password file: 11g_test2.txt, charset: alphanum, maximum length: 5, type: 11g10g
Start: 0 End: 30233088
Start: 30233088 End: 60466176
Password found: SCOTT:Cra3k:ORA11G:vostok
Elapsed 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 1 million hashes per second

Woraauthbf can also be used to crack from authentication sessions

Woraauthbf can be used in dictionary or brute force mode

SYSDBA Brute Force

```
C:\tools\brute_wright>orabrute 127.0.0.1 152
2 ora10gr2 100
Orabrute v 1.2 by Paul M. Wright and David J. Morgan:
orabrute <hostip> <port> <sid> <millitimewait>sqlplus.exe -S -L
"SYS/AASH@127.0.0.1:1522/ora10gr2" as sysdba @selectpassword.sql
```

NAME	PASSWORD
-----	-----
SYS	B024681DBF11A33E
PUBLIC	
CONNECT	
RESOURCE	
DBA	
SYSTEM	D4DF7931AB130E37
SELECT_CATALOG_ROLE	
EXECUTE_CATALOG_ROLE	
DELETE_CATALOG_ROLE	
EXP_FULL_DATABASE	
IMP_FULL_DATABASE	

<http://www.ngssoftware.com/research/papers/oraclepasswords.zip>

Listener Check

The screenshot shows the Integrity AppSentry Listener Check for the Oracle Database v2.2 application. The interface includes a sidebar with navigation options: Listener Security Check, Oracle Applications 11i Listener Security Check, SID Enumeration, TNSNAMES.ORA Security Check, and About. The main area contains input fields for Host Name or IP Address (127.0.0.1) and Listener Port Number (1522), with a note that the default is 1521. A 'Perform Listener Security Check' button is present. Below the button is a table with the following data:

Description	Result	Notes	More Information
Listener Version	✓	TNS Listener Version = 10.2.0.1.0	
Listener Password	✓	Oracle 10g, password not required (TNS-01189)	Info
Admin Restrictions	✓	Oracle 10g, no ADMIN_RESTRICTIONS (TNS-01189)	Info
Listener Logging	ⓘ	Oracle 10g, unable to check logging (TNS-01189)	Info
Local OS Auth (10g)	✓	LOCAL_OS_AUTHENTICATION=ON (TNS-01189)	Info

Works with 10gR2
Can enumerate SIDS using TNS commands
From: <http://www.integrigy.com/downloads/lisnrcheck.exe>

Sample Audit Checks Using SCUBA

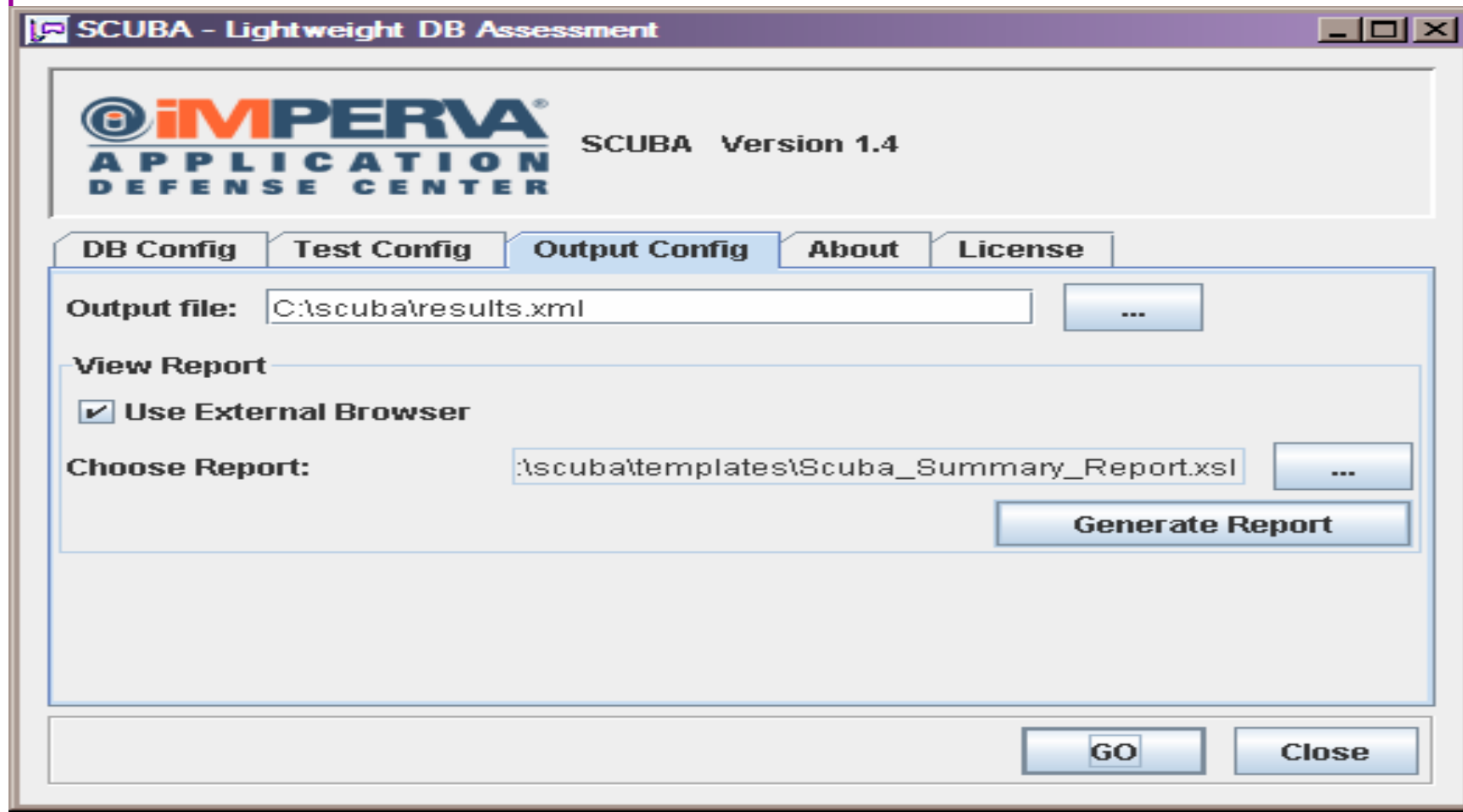
http://www.imperva.com/application_defense_center/scuba/

The screenshot shows the SCUBA - Lightweight DB Assessment application window. The title bar reads "SCUBA - Lightweight DB Assessment". The main area features the IMPERVA APPLICATION DEFENSE CENTER logo and "SCUBA Version 1.4". Below the logo are five tabs: "DB Config", "Test Config", "Output Config", "About", and "License". The "DB Config" tab is active, showing the following fields:

- DB Type: Oracle (dropdown menu)
- Host: oracle_hack_box
- Port: 1522
- DB Name: ora10gr2
- Windows Authentication
- User: system
- Password: *****

At the bottom of the "DB Config" section is a "Test Connectivity" button. A tooltip is visible over the "Test Connectivity" button, displaying the text "Type account number to be used for databases". At the bottom of the window are two buttons: "GO" and "Close".

Sample Audit Checks Using SCUBA




Sample Audit Checks Using SCUBA

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

 **The Center for Internet Security - Scoring Tool** [-] [□] [X]

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

Appendix A

Additional Settings	0.00
----------------------------	------

100% complete (269/269) [Progress Bar]

CIS Benchmark

The screenshot shows a window titled "Scoring Results" with a "File" menu. It displays two benchmark items, both with a "Status: passed".

Item #: 1.22 **Status:** passed
Configuration Item: init.ora
Action: os_authent_prefix="" (A null string)
Comments: Setting this ensures that the only way an account can be used externally is by specifying IDENTIFIED EXTERNALLY when creating a user.
Failed Results: os_authent_prefix is not a null string ("") in init.ora.

Item #: 1.23 **Status:** passed
Configuration Item: init.ora
Action: os_roles=FALSE
Comments: O/S roles are subject to control outside the database. This separates the duties and responsibilities of DBAs and system administrators.

Item #: 1.23 **Status:** passed
Configuration Item: http://www.cisecurity.org/bench_oracle.html
Action: Settings for utl_file_dir parameter should avoid certain directories (see comments)
Comments: Do not use the following settings: - "*" - Allows access to any fileAny trace file directories - Critical information could be read - "." - Allows access to the current directory Location of the core dump trace files - Critical information could be read

OScanner

```
C:\WINDOWS\system32\cmd.exe
C:\pete_finnigan_com_ltd\presentations\tools\cquire\osscanner_bin>osscanner -s 127.0.0.1 -P 1521
Oracle Scanner 1.0.6 by patrik@cquire.net
-----
[-] Checking host 127.0.0.1
[-] Checking sid (ora92) for common passwords
[-] Account CTXSYS/CTXSYS is locked
[-] Account DBSNMP/DBSNMP found
[-] Enumerating system accounts for SID (ora92)
[-] Successfully enumerated 30 accounts
[-] Account HR/HR is locked
[-] Account MDSYS/MDSYS is locked
[-] Account OE/OE is locked
[-] Account OLAPSYS/MANAGER is locked
[-] Account ORDPLUGINS/ORDPLUGINS is locked
[-] Account ORDSYS/ORDSYS is locked
[-] Account OUTLN/OUTLN is locked
[-] Account PM/PM is locked
[-] Account QS/QS is locked
[-] Account QS_ADM/QS_ADM is locked
[-] Account QS_CB/QS_CB is locked
[-] Account QS_CBADM/QS_CBADM is locked
[-] Account QS_CS/QS_CS is locked
[-] Account QS_ES/QS_ES is locked
[-] Account QS_OS/QS_OS is locked
[-] Account QS_WS/QS_WS is locked
[-] Account RMAN/RMAN is locked
[-] Account SH/SH is locked
[-] Account WKSYS/WKSYS is locked
[-] Checking user supplied passwords against sid (ora92)
[-] Checking user supplied dictionary
[-] Account WMSYS/WMSYS is locked
[-] Account XDB/XDB is locked
[-] Account WKPROXY/WKPROXY is locked
[-] Account ODM/ODM is locked
[-] Account ODM_MTR/ODM_MTR is locked
[-] Querying database for version information

C:\pete_finnigan_com_ltd\presentations\tools\cquire\osscanner_bin>dir /p
```

http://www.cquire.net/wp/?page_id=3

PL/SQL Scripts

```
Oracle SQL*Plus
File Edit Search Options Help

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

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

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

PL/SQL procedure successfully completed.

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

SQL>
```

PL/SQL Scripts (2)

```
Oracle SQL*Plus
File Edit Search Options Help
FILE NAME FOR OUTPUT [priv.lst]:
OUTPUT DIRECTORY [DIRECTORY or file (/tmp)]:
EXCLUDE CERTAIN USERS [N]:
USER TO SKIP [TEST%]:

Checking object => SYS.DBA_USERS
=====

Object type is => VIEW (TAB)
Privilege => SELECT is granted to =>
Role => APP_ROLE (ADM = NO) which is granted to =>
  User => SCOTT (ADM = NO)
  User => SYSTEM (ADM = YES)
User => CTXSYS (ADM = NO)
Role => SELECT_CATALOG_ROLE (ADM = NO) which is granted to =>
  Role => OLAP_USER (ADM = NO) which is granted to =>
    User => SYS (ADM = YES)
  Role => DBA (ADM = YES) which is granted to =>
    User => SYS (ADM = YES)
    User => SYSMAN (ADM = NO)
    User => SYSTEM (ADM = YES)
    User => TESTUSER (ADM = NO)
  Role => IMP_FULL_DATABASE (ADM = NO) which is granted to =>
    User => SYS (ADM = YES)
    Role => DBA (ADM = NO) which is granted to =>
      User => SYS (ADM = YES)
      User => SYSMAN (ADM = NO)
      User => SYSTEM (ADM = YES)
      User => TESTUSER (ADM = NO)
  Role => OLAP_DBA (ADM = NO) which is granted to =>
    Role => DBA (ADM = NO) which is granted to =>
      User => SYS (ADM = YES)
      User => SYSMAN (ADM = NO)
      User => SYSTEM (ADM = YES)
      User => TESTUSER (ADM = NO)
    User => OLAPSYS (ADM = NO)
    User => SYS (ADM = YES)
  User => SH (ADM = NO)
  Role => EXP_FULL_DATABASE (ADM = NO) which is granted to =>
    Role => DBA (ADM = NO) which is granted to =>
      User => SYS (ADM = YES)
      User => SYSMAN (ADM = NO)
      User => SYSTEM (ADM = YES)
      User => TESTUSER (ADM = NO)
    User => SYS (ADM = YES)
  User => SYS (ADM = YES)
  User => IX (ADM = NO)
```

Conclusions

- Looked at where to find Oracle security tools
- Look at the types of tools and categorized them
- Considered free and commercial tools
- Looked at protecting against Oracle Security tools
- A quick look at what Oracle provides
- Demonstrated some of the key tools that can be used
- The free tools tend to occupy the enumerate, test and scan areas

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

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