

UKOUG UNIX SIG
September 8th 2010

Oracle Security

The Right Approach (IMHO) – Part 2

By

Pete Finnigan

Updated Wednesday, 1st September 2010

Why Am I Qualified To Speak

- PeteFinnigan.com Ltd, Est 2003.
- <http://www.petefinnigan.com>
- First “Oracle security” blog.
- Specialists in researching and securing Oracle databases providing consultancy and training Database scanner software authors and vendors.
- Author of Oracle security step-by-step book; co-author of Expert Oracle practices, author of HSM/TDE Book to be published soon.
- Published many papers, regular speaker (UK, USA, Slovenia, Norway, Iceland, Finland and more).
- Member of the Oak Table Network.



Agenda - Reminder

- Two Parts to this presentation
- Background “glue”
- The correct approach (IMHO) – The message
- Exploit + reaction (a number of levels)
 - downloadable, easy
 - Realistic theft
 - Sophisticated attack
 - Data analysis
 - User Analysis
- Conclusions

Reaction From Part 1 Demo

- Access is available to the database
- Credentials are guessable
- Default accounts have access to critical data – Actually all accounts do!!
- Critical data is easy to find
- Poor, weak encryption and protection used
- This is reality, this is what Oracle database security REALLY looks like!!

Some Issues?

- OK, easy and realistic
- There are still issues, for someone to steal they still need Oracle knowledge and business knowledge
- The issue is that because “WE” (the Oracle customers) do not fix databases we make it easy to steal – the target audience for these “ADVANTAGES” is likely employees – DBA, Power users, Dev....

Data Theft

- Data theft is more likely possible due to:
 - Application abuse
 - Data not in the database
 - Data given to users
 - More....
- Oracle will not fix these issues for you, they are your responsibility!

The Defenders View

- Did our realistic attack leave evidence
- Does the DBA review these evidences?
- Audit trail
- Listener log
- redo
- More...

Live Demo 3

What if the Hacker Was Clever

- If he was clever he may take a number of different approaches
 - Stealth
 - in finding an account
 - Escalate first
 - Check identity
 - Steal the data from somewhere else

A Stealth Attack

Live Demo 4

Some Thoughts

- A data security solution must be comprehensive
- All copies of the data must be located and protected to the same level
- Theft will always occur taking the easiest approach!

The True Access To The Data

Live Demo 5

Analysing Data

- We should now be ready for “**layers**” and “**hierarchy**” being evident in this investigation
- Data is never where you think it is.
- Unless you really know where it is you cannot secure it
- Understand the access models and who can access the data

The Access Issue

- This is the number 1 Oracle security issue for me
- A database can only be accessed if you have three pieces of information
 - The IP Address or hostname
 - The Service name / SID of the database
 - A valid username / password
- A database can only be accessed at the TNS level if there is a direct route from the user (authorised or not) and the database

11gR1 has broken this with the default sid/service name feature

Access Issue 2

- At lots of sites we audit we see:
 - Tnsnames.ora deployed to all servers and desktops
 - Tnsnames.ora with details of every database
 - access to servers is open (no IP blocking)
 - Guessable SID/Service name
 - Weak passwords
- **Do not do any of these at your sites!**

The Core Problems

- Incorrect versions and products installed
- Unnecessary functions and features installed
- Excessive users / schemas installed
- Elevated privileges for most database accounts
- Default and insecure configurations
- Lack of audit trails in the database
- Data often held outside the database
- Evidence of ad-hoc maintenance

Configuration And Defaults

- Default database installations cause some weak configurations
- Review all
 - configuration parameters – checklists?
 - File permissions
- Some examples
 - No audit configuration by default (fixed in 10gR2 for new installs)
 - No password management (fixed in 10gR2 new installs)
- In your own applications and support accounts
 - Do not use default accounts
 - Do not use default roles including DBA
 - Do not use default passwords

Background Information

- Basic information must be to hand for familiarisation rather than actual use
- Vulnerabilities and exploits:
 - SecurityFocus – www.securityfocus.com
 - Milw0rm – www.milw0rm.com
 - PacketStorm – www.packetstorm.org
 - FrSirt – www.frSirt.com
 - NIST – <http://nvd.nist.gov>
 - CERT – www.kb.cert.org/vulns

Background Information 2

- Some background information we do use!
- There are a few standalone tools available
- I would start with manual queries and toolkit of simple scripts such as:
 - www.petefinnigan.com/find_all_privs.sql
 - www.petefinnigan.com/who_has_priv.sql
 - www.petefinnigan.com/who_can_access.sql
 - www.petefinnigan.com/who_has_role.sql
 - www.petefinnigan.com/check_parameter.sql
- Hand code simple queries as well

Background Information 3

- There are a number of good checklists to define what to check:
- CIS Benchmark - http://www.cisecurity.org/bench_oracle.html
- SANS S.C.O.R.E - <http://www.sans.org/score/oraclechecklist.php>
- Oracle's own checklist - http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database_20071108.pdf
- DoD STIG - <http://iase.disa.mil/stigs/stig/database-stig-v8r1.zip>
- Oracle Database security, audit and control features – ISBN 1-893209-58-X

Analysis Of Users

```

C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl
SQL> set serveroutput on size 1000000
SQL> @use
Typ      USER                Rol  Sys   Ob   Tab   PL      Status
-----
ADM      SYS                    49   200   14   870   1328   OPEN
ADM      SYSTEM                 4     5    46   153    4     OPEN
DEF      OUTLN                  1     3     1     3     1     EXPIRED & LOCKE
DEF      DIP                    0     1     0     0     0     EXPIRED & LOCKE
DEF      TSMSYS                 1     1     0     1     0     EXPIRED & LOCKE
DEF      ORACLE_OC              0     1     2     0     6     EXPIRED & LOCKE
DEF      DBSNMP                 1     4     2    20     7     OPEN
DEF      WMSYS                  3    28    12    42    52     EXPIRED & LOCKE
DEF      EXFSYS                 1     9     7    47    71     EXPIRED & LOCKE
DEF      GTXSYS                 2     7    52    43   133     EXPIRED & LOCKE
DEF      XDB                    3    10   13    23    68     EXPIRED & LOCKE
DEF      ANONYMOUS              0     1    12     0     0     EXPIRED & LOCKE
DEF      ORDSYS                 1    13   14    68    87     EXPIRED & LOCKE
DEF      ORDPLUGIN              0    10     2    10    10     EXPIRED & LOCKE
DEF      SI_INFORM              0     1     0     0     0     EXPIRED & LOCKE
DEF      MDSYS                  2    18   30   100   239     EXPIRED & LOCKE
DEF      OLAPSYS                2    13   41   126    89     EXPIRED & LOCKE
DEF      MDDATA                 2     1     0     0     0     EXPIRED & LOCKE
DEF      SPATIAL_M              3     8     0     0     0     EXPIRED & LOCKE
DEF      SPATIAL_C              3     8     0     0     0     EXPIRED & LOCKE
DEF      WKSYS                  7    59   32    56    50     EXPIRED & LOCKE
DEF      WKPROXY                0     3     0     0     0     EXPIRED & LOCKE
DEF      WK_TEST                2     0     0    13     0     EXPIRED & LOCKE
ADM      SYSMAN                 2     7    19   681   387     EXPIRED
DEF      MGMT_VIEW              1     0     4     0     0     OPEN
APX      FLOWS_FIL              0     0     6     1     0     EXPIRED & LOCKE
APX      APEX_PUBL              0     1    11     0     0     EXPIRED & LOCKE
APX      FLOWS_030             3    28   98   212   371     EXPIRED & LOCKE
DEF      OWBSYS                 10   23   43     0     0     EXPIRED & LOCKE
SAM      SCOTT                  2     1     0     4     0     OPEN
DEF      HR                      1     7     1     7     2     OPEN
DEF      OE                      2     7    14    10     1     EXPIRED & LOCKE
DEF      IX                      5    17   11    15     0     EXPIRED & LOCKE
DEF      SH                      0     0     3     0     0     EXPIRED & LOCKE
DEF      PM                      2     1    10     2     0     EXPIRED & LOCKE
DEF      BI                      0     0     8     0     0     EXPIRED & LOCKE
---      ORABLOG                2     1     1    11    18     OPEN
---      ORASCAN                0     3     0     0     0     OPEN
---      AA                      2     1     0     0     0     OPEN
---      BB                      1     0     0     0     0     OPEN
---      IMPORTER               1     0     0     0     0     OPEN
DEF      X$$NULL                0     0     0     0     0     EXPIRED & LOCKE
-----
Typ      USER                Rol  Sys   Ob   Tab   PL      Status
-----
PL/SQL procedure successfully completed.
SQL>

```

Analyse users into 2 groups

Seek to reduce the accounts (features) installed as default schemas – i.e. OEM, Intelligent agent, DIP, Samples

Analyse accounts created by “you”. Assess these in terms of what should exist

Analysing Users

Live Demo 6

Analysing Users

- Users (or rather accounts that exist in the database) provide fixed access paths to the data.
- You must understand how these accounts can access data, percentages of data, how, when
- Finally which “real people” use these accounts, share accounts....

Layers, Hierarchy, Complexity

- Each of the three examples has
 - Layers of complexity
 - Multiple requirements for one area - Users
 - Multiple paths to data
 - Multiple copies of data
 - Multiple pieces of the puzzle involved with operating system objects
 - Multiple paths to the operating system
- See the pattern now?

Conclusions

- There are a few important lessons we must learn to secure data held in an Oracle database
 - We must secure the “**data**” not the software (quite obviously we **MUST** secure the software to achieve “**data**” security)
 - We must start with the “**data**” not the software
 - We must understand who/how/why/when “**data**” could be stolen
- Oracle security is complex though because we must consider “**where**” the “**data**” is and “**who**” can access it and “**how**”
- Often there are “**layers**” and “**duplication**”
- Careful detailed work is often needed


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

Any Questions?

Contact - Pete Finnigan

PeteFinnigan.com Limited

9 Beech Grove, Acomb

York, YO26 5LD

Phone: +44 (0) 1904 791188

Mobile: +44 (0) 7742 114223

Email: pete@petefinnigan.com