UKOUG UNIX SIG
September 8\textsuperscript{th} 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.
• 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!!

09/09/2010

Copyright (c) 2008, 2009, PeteFinnigan.com Limited
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
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
  – CERT – www.kb.cert.org/vulns
• 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
There are a number of good checklists to define what to check:

Analysis Of Users

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....
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
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