

In Conjunction with Sentrigo,
Live Webinar, July 22nd 2009

The Right Method To Secure An Oracle Database

By
Pete Finnigan

Updated Tuesday, 21st July 2009

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

1

Why Am I Qualified To Speak

- PeteFinnigan.com Ltd
- Established Feb 2003
- <http://www.petefinnigan.com>
- Clients UK, States, Europe
- Specialists in researching and securing Oracle databases providing consultancy and training
- Database scanner software authors and vendor
- Author of Oracle security step-by-step book
- Published many papers, regular speaker (UK, USA, Slovenia, Norway, Iceland, Finland and more)
- Member of the Oak Table Network



24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

2

Quick Survey

- How many people here know **"where"** their key data is held?
- How many people here understand exactly **"who"** can see or **"modify"** key data?
- How many people here understand the true **"privilege model"** employed to protect **"key data"**?

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

3

Agenda

- Hardening by checklist
- Problems with checklists
- The right method
- Data flow
- Privilege/access assessment
- conclusions

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

4

Why We Need Security

- The target is often data not the DBA role
- The exploits we see on the internet work but stealing data is much more "real" and easy
- It is easy, not rocket science, no skill
- Real theft does not require complex techniques either
- What do you think happens in real life?
 - Exploits can be downloaded for free!
 - Stealing is easy because systems are open

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

5

Traditional Approach

- **Hardening by checklist – good idea?**
- A number of them available
 - SANS Step-by-step guide
 - SANS S.C.O.R.E.
 - CIS benchmark
 - DoD Stig
 - IT Governance book
 - Oracle's own checklist

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

6

Problems With Checklists

- Not many lists exist
- Mostly from same initial source or very similar
- Some structure but not good enough
 - “tip based rather than method based”
- **Doesn't focus on the data**
- Difficult to implement for a large number of databases
- CIS for instance has 154 pages

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

7

Time “vs” Clever

- Time
 - Could spend man years on even a single database
 - Finding solutions for each issue is not as simple as applying what it says in the document
- Clever
 - Solutions are needed
 - Onion based approach
 - Basic hardening in parallel

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

8

Examples Of Problems

- Two examples:
 - 1) Check 3.0.2 in CIS states “all files in \$ORACLE_HOME/bin directory must have privileges of 0755 or less – fine - but the solution states “chmod 0755 \$ORACLE_HOME/bin/*” – **good idea?**
 - 2) Solutions are not as simple as indicated. For instance fixing a weak password should include, the password, management, hard coded passwords, audit, policy....

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

9

Checklists And PII Data

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Severity	Limit #	Item Status
5.25	Encryption	Tablespace Encryption	Rationale: When a table contains a large number of columns of [PII] it can be beneficial to encrypt an entire tablespace rather than columns. Remediation: Use tablespace encryption. Audit: None	4	4	2
5.26	Radiokeys	Verify and set permissions on radiokeys file	Rationale: File permissions must be restricted to the owner of the Oracle database and its group. Ensure proper permissions are set on \$ORACLE_HOME/network/radiokeys/ocidmns.help Remediation: chmod 440 \$ORACLE_HOME Audit: ls -l \$ORACLE_HOME	5	1	5
5.27	Sqlnetora	\$ORACLE_HOME/network/admin/sqlnetora	Rationale: Oracle documentation is required for checking CDBs for client certificate authentication. Rowlock certificates are listed in the directory of the CDB database.	2	2	5

Some mention of data BUT not focused

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

10

Checklists And Special Data

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Severity	Limit #	Item Status
1.1.1	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.2	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.3	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.4	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.5	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.6	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.7	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.8	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.9	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.10	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.11	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.12	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.13	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.14	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.15	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.16	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.17	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.18	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.19	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5
1.1.20	Database user accounts	Identify and remove unnecessary database user accounts	Rationale: Database user accounts should be limited to those required for the database. Unnecessary accounts should be removed to reduce the attack surface.	5	1	5

No special data mentioned at all

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

11

The Right Method To Secure

- Start with **“the data”**
- Understand **“data flow”** and **“access”**
- Understand the problem of securing **“your data”**
- **Hardening should be part of the solution BUT not THE solution**
- Checklists do not mention **“your”** data

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

12

Complex But Simple Solutions

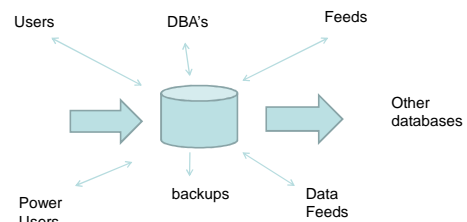
- Overarching solutions
- Remove all types of access from data
- Ensure only those who should see, can see the data
- Unfortunately its not simple as there are:
 - Many paths to the data
 - Many copies of data
 - Data stored or in transit that is accessible
 - Data copied outside of the database

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

13

Architecture



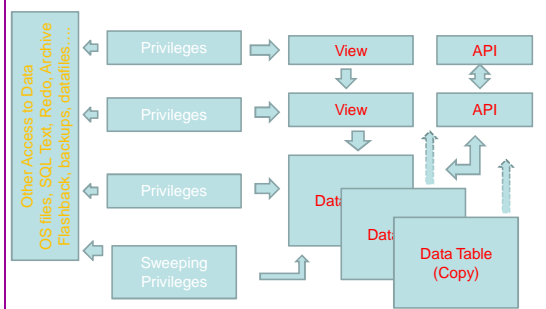
Identify each type of person and a sample account for each

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

14

Data Access Models



24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

15

Data Access Is Not "Flat"

- Data model is not flat – remove the blinkers
- Access rights are also not flat
- Data is often replicated
 - In other tables – in interfaces – flexfields ...
 - Indexes
 - Shared memory
 - Data files
 - Operating system
 - Many more...

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

16

How / Who

- The data must be identified (found?)
- The access paths must be found
- The "people" – real people identified
- Map to database users
- Assess who can access data and how
- Only now can we hope to secure data

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

17

Securing Data

- We are going to investigate in depth the issues around a simple credit card table
- We need to
 - find the credit card table
 - Find duplicate copies
 - Assess who can access all
 - Other places the data exists
 - More...
- Even these issues are only the "**tip of the iceberg**" though!
- Lets dig deeper

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

18

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

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

31

Quick Survey – Again!

- How many people know **"where"** their key data is held?
- How many people understand exactly **"who"** can see or **"modify"** key data?
- How many people understand the true **"privilege model"** employed to protect **"key data"**?

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

32

PeteFinnigan.com Limited

create or replace function log_error_path
return varchar2 as
begin
return 'PeteFinnigan.com Limited
Oracle Security Expertise
http://www.petefinnigan.com';
end;

Any Questions?

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

33

PeteFinnigan.com Limited

create or replace function log_error_path
return varchar2 as
begin
return 'PeteFinnigan.com Limited
Oracle Security Expertise
http://www.petefinnigan.com';
end;

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

24/07/2009

Copyright (c) 2009
PeteFinnigan.com Limited

34