

Problems With Checklists

- Not many checklists exist for Oracle databases
- Most are from same initial source or are very similar
- Some structure there but not good enough
 - “tip based rather than method based”
- Lists don't focus on securing the data
- Difficult to implement for a large number of databases
- CIS for instance has 158 pages

12/03/2010

Copyright (c) 2010
PeteFinnigan.com Limited

7

Time “vs” Clever

- Time solution
 - 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 solution
 - Technical solutions need to be specified
 - Onion based approach is good
 - Basic hardening in parallel

12/03/2010

Copyright (c) 2010
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/*” – is it a good idea?
 - 2) Solutions are not as simple as indicated. For instance fixing a weak password should also include, fix the password, management, hard coded passwords, audit, policy....

12/03/2010

Copyright (c) 2010
PeteFinnigan.com Limited

9

Checklists And PII Data

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Severity	CVSS	Check	Fix
3.25	Encryption	Tablespace Encryption	Rationale: Users who have complete a large number of columns of data can be vulnerable to encrypt an entire tablespace other than columns. Remediation: Use tablespace encryption... Audit: None	1	4		
3.26	Filesystem	Verify and set permissions on critical log file	Rationale: File permissions must be restricted to the owner of the Oracle software and the group Oracle owner permissions are set on \$ORACLE_HOME/bin/permissions/permissions. Remediation: chmod 411 \$ORACLE_HOME/bin/permissions/permissions. Audit: ls -l \$ORACLE_HOME/bin/permissions/permissions	1	5		
3.27	Database	SQL*NET_REMOTE_LOGIN_FILE	Rationale: Oracle installation is required to be able to connect to other Oracle instances. Remediation: Set the parameter to a secure location. Audit: sqlnet.ora	1	5		

12/03/2010

Copyright (c) 2010
PeteFinnigan.com Limited

10

Checklists And Special Data

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Severity	CVSS	Check	Fix
3.1	Database	SQL*NET_REMOTE_LOGIN_FILE	Rationale: Oracle installation is required to be able to connect to other Oracle instances. Remediation: Set the parameter to a secure location. Audit: sqlnet.ora	1	5		

12/03/2010

Copyright (c) 2010
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

12/03/2010

Copyright (c) 2010
PeteFinnigan.com Limited

12

Complex But Simple Solutions Needed

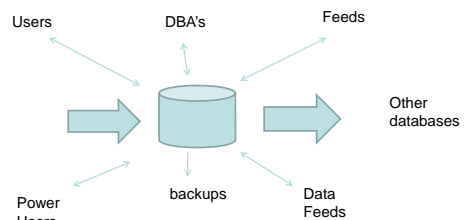
- Overarching solutions are needed
- Remove all types of access from the data
- Ensure only those who should see, can see the data
- Unfortunately it's not that simple as there are:
 - Many paths to the data
 - Many copies of data
 - Data stored or in transit that is accessible
 - Data copied outside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

12/03/2010

Copyright (c) 2010
PeteFinnigan.com Limited

13

Understand Architecture



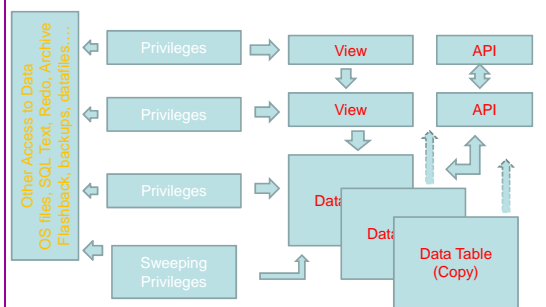
Identify each type of person and a sample account for each

12/03/2010

Copyright (c) 2010
PeteFinnigan.com Limited

14

Data Access Models



12/03/2010

Copyright (c) 2010
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...

12/03/2010

Copyright (c) 2010
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 these to database user accounts
- Assess who can access data and how
- Only now can we hope to secure data

12/03/2010

Copyright (c) 2010
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 details table
 - Find duplicate copies of credit card data
 - Assess who can access all of the data
 - Look for other places the data exists
 - More...
- Even these issues are only the "**tip of the iceberg**" though!
- Lets dig deeper

12/03/2010

Copyright (c) 2010
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

12/03/2010

Copyright (c) 2010
PeteFinnigan.com Limited

31

PeteFinnigan.com Limited

Oracle Security Expertise

Any Questions?

12/03/2010

Copyright (c) 2010
PeteFinnigan.com Limited

32

PeteFinnigan.com Limited

Oracle Security Expertise

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

12/03/2010

Copyright (c) 2010
PeteFinnigan.com Limited

33