

Oracle Database Security and Audit

Beyond Checklists

Agenda

- Tools to use for the audit

Basic requirements

- Do not impact performance
- Do not access customer data
- Do not create objects in the database
- Do not cause a license violation for the customer
- Do not adversely affect the file system

Oracle security information

- Many sources
- Usual places
 - Oracle security information
 - Post installation docs
 - Metalink
- Database internals

New features



Remember -
new features = new vulnerabilities

Copyright © 2014, Reidy Database Consulting, LLC

Oracle security documentation: http://docs.oracle.com/cd/E16655_01/server.121/e17609/toc.htm

Oracle post installation docs: http://docs.oracle.com/cd/E16655_01/install.121/e17720/post_inst_task.htm#LADBI7744

Metalink:

Security Checklist: 10 Basic Steps to Make Your Database Secure from Attacks (Doc ID 1545816.1)

Project lockdown: <http://www.oracle.com/technetwork/articles/index-087388.html>

Tools

- Discovery tools
- Enumeration tools
 - Users - OAK toolkit, nmap
 - SID guessing - OAK toolkit, THC, nmap
 - Listener enumeration - nmap, WinSID, Isnrcheck

These tools are not suitable for audits, but they are interesting to know about.

Copyright © 2014, Reidy Database Consulting, LLC

OAK toolkit - <http://www.databasesecurity.com/dbsec/OAK.zip>

nmap - <http://nmap.org/download>

THC - <https://www.thc.org/thc-hydra/>

WinSID - <http://www.vulnerabilityassessment.co.uk/winsid.htm>

Isnrcheck - <http://www.integrigy.com/security-resources/downloads/Isnrcheck-tool>

Tools (2)

- Testing tools
 - Password crackers - orabf, woraaauthbf, Cain & Abel
 - Listener enumeration - nmap, tnsrmd
 - Kali or Backtrack Linux

These should be suitable for audits, but they do not do the whole job.

Copyright © 2014, Reidy Database Consulting, LLC

orabf -

woraaauthbf - http://www.soonerorlater.hu/index.khtml?article_id=513

tnsrmd - <http://www.jammed.com/~jwa/hacks/security/tnsrmd/tnsrmd>

Cain & Abel - <http://www.oxid.it/cain.html>

Tools (3)

- Scanners - free
 - Rorascanner
 - Scuba
 - oscanner
- Scanners - commercial
 - AppDetectivePRO
 - PFLCScan
 - others

Rorascanner – <http://rorascanner.rubyforge.org>

Scuba – http://www.imperva.com/products/dsc_scuba-database-vulnerability-scanner.html

oscanner – <http://www.cqure.net/wp/tools/database/oscanner/>

AppDetectivePRO – <http://www.appsecinc.com/index.php/products/appdetectivepro>

PFLCScan – <http://www.pflcscan.com>

Security books

- SANS – Oracle Security Step-by-Step (Pete Finnigan)
- Oracle Privacy Security Auditing (Arup Nanda)
- Effective Oracle database security by design (David Knox)
- Applied Oracle Security (David Knox – et al)
- Oracle hackers handbook (David Litchfield)
- Oracle Forensics (Paul Wright)
- Database Hackers Handbook (David Litchfield)
- Security, Audit and control features – Oracle database 3rd edition - ISACA
 - Auditing Oracle Databases Using CAATs - Ian Cooke

Use SQL*Plus

- Easy scripting language
- Runs against all Oracle database versions
 - Scripts
 - find_all_privs.sql
 - who_has_role.sql
 - who_has_priv.sql
 - who_can_access.sql
 - check_parameter.sql
- Easy to automat into your own scanner

All SQL*Plus scripts mentioned in this slide can be downloaded from <http://www.petefinnigan.com/tools.htm>

Modified versions included with the course

Q&A