Reidy Database Consulting, LLC Database Security and Risk Assessment

Oracle Database Security and Audit

Beyond Checklists

Convisht © 2014 Reidy Database Consulting 11

Reidy Database Consulting, LLC Database Security and Risk Assessment

Agenda

• Tools to use for the audit

Copyright © 2014, Reidy Database Consulting, L

Reidy Database Consulting, LLC Database Security and Risk Assessment

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

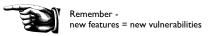
Convictor © 2014 Reidy Database Consulting 11

Reidy Database Consulting, LLC Database Security and Risk Assessmen

Oracle security information

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

New features



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

Reidy Database Consulting, LLC Database Security and Risk Assessmo

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.

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

Reidy Database Consulting, LLC Database Security and Risk Asses

Tools (2)

- Testing tools
- Password crackers orabf, woraauthbf. Cain & Abel
- Listener enumeration nmap, tnscmd
- Kali or Backtrack Linux

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

orabf -

woraauthbf - http://www.soonerorlater.hu/index.khtml? article id=513

tnscmd - http://www.jammed.com/~jwa/hacks/security/ tnscmd/tnscmd

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

Reidy Database Consulting, LLC Database Security and Risk Assessmen

Tools (3)

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

yright © 2014, Reidy Database Consulting, LLC

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
PFCLScan - http://www.pfclscan.com

Reidy Database Consulting, LLC Database Security and Risk Assessme

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

pyright © 2014, Reidy Database Consulting, LLC

Reidy Database Consulting, LLC Database Security and Risk Assessmen

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

Copyright © 2014, Reidy Database Consulting, LL

_			
	Reidy Database Consulting, LLC Database Security and Risk Assessment		
		O 0 A	
		Q&A	