Oracle Database Security and Audit

Beyond Checklists

Copyright © 2014, Reidy Database Consulting, LLC

Agenda - History of Oracle

- History of Oracle and its security evolution
- Current state of Oracle security
- Key security issues

Copyright © 2014, Reidy Database Consulting, LLC

Learning objectives

- Understand Oracle security evolution
- Understand current state of Oracle security
- What is wrong in database security

Copyright © 2014, Reidy Database Consulting, LLC

Reidy Database Consulting, LLC
Database Security and Risk Assessment

Why "beyond checklists"?

- There are many checklists
  - DOD STIG
  - Oracle's checklist
  - SANS S..C.O.R.E
  - CIS Oracle Benchmark

Copyright © 2014, Reidy Database Consulting, LLC

DOD Oracle STIG: http://iase.disa.mil/stigs/app_security/database/oracle.html
Oracle security checklist: http://www.oracle.com/technetwork/database/security/twp-security-checklist-database-1-132870.pdf
SANS S.C.O.R.E.: http://www.sans.org/score/oraclechecklist.php
CIS Oracle Benchmark: https://benchmarks.cisecurity.org/tools2/oracle/CIS_Oracle_Database_Server_11_-_11g_R2_Benchmark_v1.0.0.pdf

Reidy Database Consulting, LLC
Database Security and Risk Assessment

Checklist shortcomings

- They are a hardening stance
- There give a false sense of security
- They are general in nature

They do not know your organization or your data!

Copyright © 2014, Reidy Database Consulting, LLC

Reidy Database Consulting, LLC
Database Security and Risk Assessment

Going beyond

- In this seminar I will be showing you why we need to get out of the checklist mentality
- Think about the data and its access

Copyright © 2014, Reidy Database Consulting, LLC

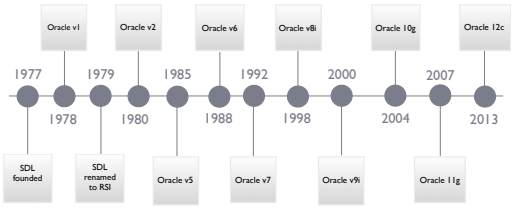
Preliminaries

- No system is 100% secure!
  - If it were100% secure, it would not stay that way
- Oracle is complex
- Oracle is an open system
- Oracle security is complex
  - The more you do it, the easier it will become

I am going to try and simplify things

Copyright © 2014, Reidy Database Consulting, LLC

Oracle Security Evolution



Copyright © 2014, Reidy Database Consulting, LLC

http://en.wikipedia.org/wiki/Oracle_Corporation#Overall_timeline

Software Development Laboratories (SDL) formed by Larry Ellison, Bob Miner, Ed Oates.

Oracle v1 never released. Oracle was a code name of a CIA project all had worked on at Ampex Corp.

Oracle v2 purchased by Wright Patterson AFB. This version had rudimentary passwords.

Current security features

- Users / Schemas
- Roles
- System privileges
- Object privileges (on all objects, tables, packages, views…)
- Password and resource management
- Audit features via
  - Core audit
  - Fine Grained Audit (FGA)
  - Triggers
- Identification and authentication
- Virtual Private Database (VPD)
  - Oracle Label Security (OLS)
- Built-in encryption – for database and file system (TDE)
- Network encryption solutions

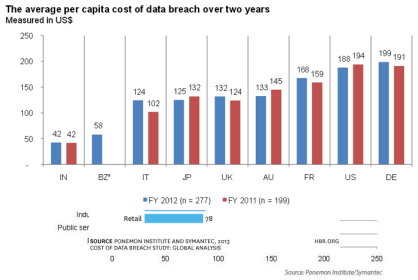
Copyright © 2014, Reidy Database Consulting, LLC

Why do we care about Oracle security?

- Oracle houses and processes the data
- Hackers want the data

Copyright © 2014, Reidy Database Consulting, LLC

The cost of data breaches



Copyright © 2014, Reidy Database Consulting, LLC

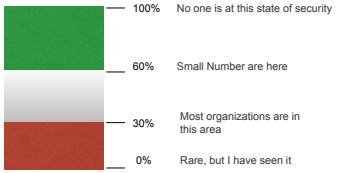
Data breach study: https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

What has gone wrong with database security

- Networked applications
  - Network security doesn't protect an Oracle database
- Requirements to protect data (particularly financial data, personally identifiable data, health information, intellectual property, etc)
  - Legislation and regulations are now prevalent in a lot of market sectors
- Most database installations are default with little or no attempt at hardening
- Oracle doesn't make it easy to secure Oracle as they provide an "open" installation by default
  - All functions are features are available to almost all users
- The insider threat is more real than the external threat

Copyright © 2014, Reidy Database Consulting, LLC

Existing state of database security



Copyright © 2014, Reidy Database Consulting, LLC

Why can data be stolen

- Security bugs
  - Patching can fix these
- Configuration issues
  - More complex - applications can break
- Feature overload
  - Software installed
  - Schemas installed
- Defaults
  - Passwords
  - Privileges

Copyright © 2014, Reidy Database Consulting, LLC

Patching

- A major issue plaguing Oracle customers
- Oracle releases quarterly security patches
- Many do not apply security patches
  - Run old versions or unsupported patch sets of the database software
- This is a very small part ofsecuring Oracle and what we are learning on this course covers the rest

Copyright © 2014, Reidy Database Consulting, LLC

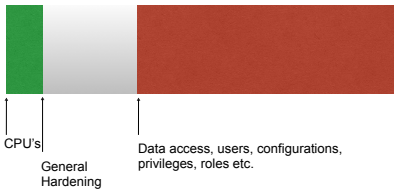
Patching is a very important activity. But is not a panacea to security. It will address known security bugs (most times).

Exploits

- Oracle has fixed hundreds of security bugs
- Each Critical Patch Update (CPU) fixes large numbers of database security bugs
- Each CPU often is followed closely by exploit code published to sites such as http://www.exploit-db.com/
- Oracle also silently fix bugs in each CPU (not listed in the advisories)
- A number of commercial companies and researchers reverse engineer the patches to find and write exploits
- Because of the nature of most exploits there are an infinite number of possible exploits that can be written
  - IDS evasion
  - Injection (SQl and PL/SQL)

Copyright © 2014, Reidy Database Consulting, LLC

Divide the issues



Copyright © 2014, Reidy Database Consulting, LLC

Security issues

- Wrong products installed – EE when SE would do
- Default installations – too many software features installed
  - Default schemas installed – default install
- Passwords weak – defaults, pwd=user, dictionary words, too short
- Audit not enabled
- Default configurations
- Bad user privilege design – least privilege principal not followed
- DBA's use SYS and SYSTEM and share accounts
- The database can be accessed from anywhere using TNS

Copyright © 2014, Reidy Database Consulting, LLC

Q&A

Copyright © 2014, Reidy Database Consulting, LLC