Course Description

This course is a one day seminar that teaches the delegates how to perform simple yet cost effective security measures where appropriate in their databases. This is with a single goal to reduce the risk to attack, misuse and abuse of data held in their Oracle databases.

The class starts the day with a detailed penetration test of our sample database and its applications and shows how the database platform itself can be attacked as well as data stolen or accessed in the database. The day goes on to harden the database in detail with lots of practical examples and the day is completed by a re-test of the attacks to show how much more secure the database has become.

Course Goals

Most databases that are built are unfortunately designed with a bigger focus on performance, functionality and availability with security being the poorer cousin. If you are charged with designing, building or managing an Oracle database then you must consider; what are the risks to the security and validity of "your data". This class focuses on structured hardening and locking down of key data and key activities in your databases with some free tools and examples to help you improve your skills in securing data in an Oracle database.

Course Duration

The class is One Day 9am to 5pm and is instructor lead with demonstrations

Course Location

The course can be held at your site or students can attend a public class. No public classes are scheduled at present. Details of on-site requirements are provided during the booking process

Course Pre-Requisites

The class is intended for DBA's and security professionals who should appreciate the techniques used to lock down and secure the database. Developers will also appreciate some of the code based techniques used in context based security

Course Material

The student will receive a URL to download a zip file that includes:

- The course notes as PDF files
- Free PL/SQL tools and scripts
- All of the examples used as SQL and PL/SQL scripts

Course Outline

The course outline is as follows

- Introduction
  - Where does lock down fit in the data security process
- Attack and Defence
  - Penetration testing of the database and applications
  - Review design choices and consequences
  - Review data leakage and consequences
  - Analyse the results and Audit trails
- Hardening The Operating System and Network
  - What is hardening
  - Operating system hardening
    - Defaults, clean up, lock down, permissions
  - Network hardening
    - Defaults, listener
- Patching and Hardening the Database
  - Database Security patches and hardening
  - Setting parameters
  - Controlling privileges on code and objects
  - Default users and functionality
- User based Security
  - User Analysis and account security
  - Profile design
  - Privilege analysis, separation and duplication
  - DBA roles and access
  - Third party and developer access
- Data and Context Based Security
  - Data access privileges
  - Account provisioning
  - Resource Access
  - Context based security and Break glass
- Strong Audit Solutions
  - Audit Levels and design
  - Policy Based database Audit
  - PFCLATK a toolkit
- Finishing Up
  - The journey today
  - Hacking the demo system again
  - Review
  - Is it secure?
  - Do we detect attacks?

This course is fast paced and very interesting and is delivered by one of the most well known experts in database security. Pete Finnigan created the SANS Oracle security step-by-step guide and the CIS Oracle benchmark used by NIST, USA DoD and more is a reference to secure Oracle databases. Pete worked out the mechanisms that Oracle used to protect PL/SQL and showed how they can be easily defeated at the Black Hat conference in Las Vegas in 2006. Pete has published multiple books on databases security and speaks and publishes papers regularly. His company also produces the tool PFCLScan used to protect Oracle databases.

