Course Description

This course is a one day seminar that gives the delegates an appreciation of what is involved in securing the Oracle database platform and also securing data in an Oracle database.

The class starts the day with the basics; what is security and what is data security? - We go on to discuss why your data leaks and is insecure before examining some sample exploits and techniques used by attackers. What are the basics of Oracle security; good design, data domains, data security and user security. We go on to discuss secure coding as well as audit trail design and how to deal with an incident or forensic analysis. We complete the day with looking at policy creation, tools and options available as well as defining a strategy

Course Goals

The aim of the class is for students to get an appreciation of where the risks lie in processing and use of data in their organisations Oracle databases. The goal is to lay out all of the major areas of issue and also possible solutions. The students will cover:

- How data is stolen and stored weakly in an Oracle database
- How to plan for data security and to develop and create a data security policy
- How to focus your efforts on securing the right data using the right solutions

Course Duration

The class is One Day 9am to 5pm and is instructor lead with some 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, Developers, security professionals, IT management and anyone involved in deploying, developing and maintaining Oracle databases. No detailed technical knowledge of Oracle databases is necessary in advance.

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

- Introduction
    - What is Oracle Security?
    - What is data security?
    - Threats, risks, counter measures
    - Pro-Active or Reactive?
- Data Loss and Attacks
    - How does Oracle process your data?
    - What are the data issues that affect Security
    - How do your decisions make your data insecure?
    - How do people attack your database and data
- The Basics
    - Design security, don't make it up!
    - Data domains
    - Data security
    - User security
    - Context based security
- Secure Coding
    - What is SQL Injection
    - What other types of code attacks are there
    - Secure coding techniques
- Design Audit Trails
    - Designing Audit Trails
    - I want to know
    - Options available
    - Management
    - Reporting and alerts
- Attacks and Forensics
    - Incident response approach and possible tools to use
    - Where to find evidence
    - What if I have no audit?
    - What to do next
- Choosing The Right Approach to Secure Your Databases
    - Creation of a Policy
    - The security features of the Oracle database
    - Additional cost options
    - Third party options and products
    - What if you do not license features
- Finishing Up
    - The journey today
    - Automated testing and where to learn more

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.