Course Description

This course is a one day seminar that gives the delegates an appreciation of what is involved in responding to a serious security incident in their Oracle database.

The class starts the day with the basics; what is a threat, what is an incident, what are forensics - We go on to discuss how to gather artefacts from an Oracle database; we discuss and lay out a suitable incident response approach. The class then introduces a compromised application and Oracle database and we work through live incident response and data gathering against this sample system. This is followed by a detailed forensic analysis to investigate what happened and answer the who, what, where and how questions. The investigation is then confirmed by comparing with exactly what the hacker did do. The day ends with a look at what to do next to secure and audit your databases and to make them ready for any incident and response.

Course Goals

The aim of the class is for students to get an appreciation of what to do if one of their Oracle databases is breached. The goal is to lay out all of the major areas of issue and also possible solutions. The students will cover:

- How to formulate an incident response plan
- How to gather data and investigate a breached database
- How to focus the analysis to understand what the hacker did and why
- How to plan to avoid an incident in the first place

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
  - Types of attack
  - What is an incident?
  - What is database forensics?
  - Chain of custody
- Gathering Artefacts
  - Heisenbergs uncertainty principal of Oracle
  - Audit or no audit trail?
  - Detecting READ actions
  - Identity and accountability
  - Time
  - Database artefacts
  - Non-Database artefacts
  - Deleted data
- Incident Response Approach
  - Create an incident response approach
  - Create an incident coordinator
  - Create an incident response team
  - Create an incident response toolkit
- Reacting to an Incident
  - Sample attack system
  - What not to do
  - Incident verification
  - Collecting artefacts
  - Disconnect or shutdown
  - Live response
- Forensic Analysis
  - Example analysis
  - Post analysis
  - How did he get in?
  - What rights?; what did he see?; what did he change?;What could be have done?
- What did the Hacker do?
  - Lets show what the hacker actually did
  - Compare the forensic analysis to the actual attack
- Finishing Up
  - Planning
  - Think about database security
  - Enable sophisticated audit trails

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.