

Course Structure

- 8 lessons of 1.5 hours each
- 09:00 – 10:30 = lesson 1
- Coffee
- 10:45 – 12:15 = lesson 2
- Lunch
- 13:15 – 14:45 = lesson 3
- Coffee
- 15:00 – 16:30 = lesson 4
- I will stay around after class
- Day 2 follows the same structure

Lesson 1 – Start From The Beginning

- Introduction to Oracle security
 - Overview of the current key issues
 - Course structure
- First principals
- Test environment
- Oracle structure with a security slant
 - Database logical structure
 - Database physical structure
 - Key components
 - Basic tools
 - SQL and PL/SQL

Lesson 2 – Information And Exploits

- Background to Oracle Security
 - Information
 - Tools
 - Checklists
- Why perform a security audit on an Oracle database?
 - Internal threats
 - Power users
 - DBA's
 - Bugs
- Exploits and attack vectors
 - Configuration
 - SQL Injection
 - Data theft

Lesson 3 – Planning And Starting The Audit

- Planning an audit
 - Environment
 - Tools
 - Planning
 - Expected results
- Preparing for an audit
 - Gathering tools
 - Preparing
 - Keep it neutral
- Starting the audit
 - Organising connections
 - Understand the architecture

Lesson 4 – Interview, Base Data And Users

- Interview key staff
 - Backups
 - Resilience
 - Access methods
- Base data
 - Versions
 - Patches
 - Software installed
- Audit users
 - Enumeration
 - Password strength
 - Profiles

Lesson 5 – Operating System And Network

- Review and audit the operating system
 - Looking for passwords
 - Data leakage
 - Configuration
 - Permissions
- Review the Oracle networking
 - Passwords
 - Listener configuration
 - Permissions
 - Logging

Lesson 6 – Database Configuration

- Review the database configuration
 - Roles
 - Profiles
 - Resources
 - Permissions on objects
 - Code
 - Privileges
 - Parameters

Lesson 7 – Specialist Considerations

- Step 1 - Review critical data
 - Reviewing critical data
 - Authentication
 - Personally Identifiable Information
 - Credit Cards
 - Problems with special data
- Step 2 - Review audit trails
 - Oracle audit facilities
 - Audit the audit trails
 - Audit configuration
 - Audit data storage
 - Logins – failed and successful
 - Listener logs

Lesson 8 – Writing Up The Audit

- Analyse the data found
- Risk assessment
- Identify vulnerabilities
- Document the audit
- Correction strategy
- Longer term and policies
- Automate the process
 - Tools
 - Monitoring
- Conclusions