Oracle Privacy Security Auditing
Course Summary

Description
Securing your Oracle Database is no longer an option; it's a necessity in today's environment where laws and regulations such as SOX and mandates such as PCI demand, not expect compliance. How do you start and, more important, where do you start? This course teaches some core concepts in Oracle Database Security for DBAs and Developers to prepare them to meet the challenges of the new rulebook in security and compliance .Attendees will learn all about Oracle Security with the working examples of threats and vulnerabilities and real life advice on mitigation plans and action points. The content is addressed to60% DBA, 40% Developer/Architect and about 30% overlapping all areas. All concepts are explained with live demonstrations and series of scenario analysis.

Objectives
At the end of this course, students will have an understanding of:

- Various components of Oracle security
- Grouping security needs by priority and effort
- Various vulnerabilities and threats
- Mitigation plans for each
- Audit buster tips
- Working scripts and tools for above

Topics

- Database Security Primer
- Different Areas of Insecurity in Oracle Context – Stolen Backup, Perimeter Breach, Buffer Overflow, etc.
- Listener Vulnerabilities and Security
- Admin Restrictions and Password Protection
- Buffer Overflow Concepts
- Modes of Denial of Service Attacks
- Attacks on the Live Database
- Securing the Different Oracle Executables – oracle, tnslsnr, etc.
- Managing SYSDBA Privileges and Oracle Password File
- Managing Passwords – Practical Insights
- Identifying and Eliminating Default Users
- Eliminate Default Passwords (e.g. TIGER for SCOTT)
- Change Passwords for Key Users (DBSNMP, SYSMAN)
- Identifying "Sweeping" Privileges
- Tablespace Quotas
- Common Misconceptions –
- SELECT_CATALOG_ROLE and SELECT ANY DICTIONARY
- Identifying "Seemingly Innocuous Privileges"
- Identifying Potentially Dangerous Privileges and
- Supplied Packages
- Special Cases – UTL_FILE_DIR Initialization Parameter
- Identifying and Eliminating Indirect Grants
- Identifying Listener Break-ins
- Hiding Passwords
- PL/SQL Wrapping – 10gR2 way included
- Schema Change Control
- Restricting SQL*Plus
- SQL*Plus Product Profiles
- Different Types of Roles – Common, Password Protected and Secure Application Roles
- Mining Information from Listener Logs
- Building a User Profile from the Listener Logs
- Simple Auditing
- Auditing for Future Objects
- Identify Access Violations or Break-in Attempts
- Auditing on Objects – by Session and by Access
- Using a Secure Application Authentication Mechanism
- Node Validation
- Track DDLs from Log Miner
- Protecting Backups – Encrypting Backups

Prerequisites
Students should have Knowledge of Oracle Database– any level.

Duration
One day

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically