

## **COURSE TITLE: SECURING ORACLE DATABASE**

Course Instructor: Alexander Kornbrust

Course Duration: 5 days

Minimum Class Size: 5

Course Fees: S\$7,000 per students

Course Pre-requisites: Students should have a good knowledge of Oracle databases

Course Material: English course notes, Scripts, Free Security Software

### Course Outline:

#### Oracle Security Information

- Oracle Security related Websites (Where to find Exploits, Gossip....)
- Books (Useful Oracle Security books)
- Metalink Hacking (Find unknown/unpublished security bugs in Metalink)
- Google Hacking of Oracle Technologies
- Yahoo Hacking of Oracle Technologies
- Analysing Oracle Security Patches
- Where to buy unpublished Oracle Security Bugs

#### Security Basics

- Secure Oracle Architecture (Client, Server, Application Server, Backup/Recovery...)
- Oracle Security Features (Audit, Encryption, ASO, VPD, OLS...)
- Encryption (Concepts, Network, Database...)
- Privileges
- Audit (Concept, what...)
- Forensics
- D.o.S. - Denial of Service (Concepts, TNS-Listener, database, database user, oid...)
- Buffer Overflows (Concepts, Packages, SQL functions...)
- SQL Injection (Concepts, Packages, Trigger, Webapplication...)
- Cross Site Scripting (Concepts, How to use...)
- Tools (Scripts, Oracle Security Scanner, Free and commercial software ...)

#### Database

- Attack Scenarios
- Overview Security Windows (Services, Patches...)
- Overview Security Unix (X11, Services, Patches...)
- File Permission (Common Issues, Become Root... )
- Listener (TNS, MTS, XMLSDB, Exploits, Securing Listeners...)
- Network Sniffing & Tracing (Ethereal, Tracing, ASO...)
- Reading and stealing files (Export, archive, utl\_file, dbms\_lob...)
- Creating Files ( utl\_file, external tables, dbms\_advisory, Java...)
- Oracle Database Passwords (Brute Force Cracker, Password Algorithm, hashkeys...)
- Other Oracle Passwords (modplsqli, CMDSK, changing, decrypting...)
- Execute OS commands (Java, Extproc, undocumented Procedures...)
- Database Encryption (Decrypt Data, Steal encryption keys, Circumvent Encryption, sort\_area\_size, Reverse Engineering Key Algorithms)
- PLSQL (Wrapping, Unwrapping PLSQL, Patching wrapped procedures, ...)
- XMLDB (D.o.S, XSS, ...)
- Backdoors (How to Implement, Find)
- Become DBA (several ways to become DBA)
- Components
  - HTMLDB
  - XMLDB

- Enterprise Manager
- iSQLPlus
- OID
- Hardening Oracle Database (Approach, where to start, top-5-issues, Keep the database secure...)
- Oracle Clients
  - Attack Scenarios
  - Passwords & Accounts (Handling, Roaming, Decryption, ...)
  - Client Startup Files
  - SQL Logging
  - Temp Files
  - Analysing various Oracle Clients
  - Using Windows PE / Knoppix (Create own Oracle Boot-CD)
  - Hardening Oracle Clients
- Application Server
  - Attack Scenarios
  - Oracle HTTP Server (Apache)
  - Oracle Forms Server (SQL Injection, OS execution...)
  - Oracle Reports Server (SQL Injection, OS execution...)
  - Oracle Webcache
  - Oracle Portal (SQL Injection)
  - Hardening Oracle Application Server
- Advanced Topics
  - Oracle Rootkits (Concepts, Create invisible users, modify packages, ...)
  - Oracle Viruses (Concepts)
  - Oracle Worms (Concept)
  - Oracle Firewalls
  - Oracle Phishing
  - Oracle Patch Modification