Course Outline

Expanded Security Workshop for IBM i, iSeries, AS/400

Course Summary

Description

This class provides a comprehensive treatment of IBM i (iSeries, AS/400) security concepts along with practical instruction for implementing those concepts. Special Tips and Techniques will be provided throughout the class. During the supervised Hands-On lab sessions, the student will audit and detect faulty implementations that could compromise the system. This workshop is designed for those dealing with system setup and administration, including system administrators, security officers, and IT Auditors. Expanded hands-on lab exercises reinforce the concepts presented. The workshop is also recommended for technical support personnel and those staff members who set standards/policies for Application Development and Change Control.

Topics

- IBM i Technical Overview
- System Level Security
- All About User Profiles
- Object Oriented Architecture
- The Security Toolkit
- Work Management Security
- Application Security
- Network Security and Logging
- Auditing Capabilities
- IBM i Navigator Security

Audience

It is recommended for technical support personnel and those staff members who set standards/policies for Application Development and Change Management.

Prerequisites

There are no prerequisites for this course.

Duration

Four days

Course Outline

Expanded Security Workshop for IBM i, iSeries, AS/400

Course Outline

I. IBM i Technical Overview
- A. Menus, Commands
- B. Finding Commands
- C. OS Architecture

II. System Level Security
- A. Security System Values
- B. Security Levels
- C. Password Levels
- D. Protecting SST and DST services
- E. Encryption Options

III. All About User Profiles
- A. Working with User Profiles
- B. Special Authorities
- C. Limit Capabilities
- D. User Classes
- E. Group Profiles
- F. Reporting *Outfiles w/ Query/SQL
- G. Object Ownership
- H. Adopted Authority
- I. Finding Back-door Programs
- J. Preventing User Profile Hijacking
- K. Common mistakes in User Profiles

IV. Object Oriented Architecture
- A. A File is a File a Program is a Program
- B. Library and Object Authorities
- C. Security Commands for Objects
- D. Security Commands for IFS Objects
- E. Authority Shortcuts
- F. Authorization Lists
- G. Common Misunderstandings

V. The Security Toolkit
- A. SECTOOLS Menu Options
- B. Security Jobs in the Job Scheduler

VI. Work Management Security
- A. Sign-on Screen Vulnerabilities
- B. QSYSOPR Message Queue Authority
- C. Library List Vulnerabilities
- D. Checking for Trojan Horse Programs
- E. Job Description Vulnerabilities

VII. Application Security
- A. Vendor supplied schemes
- B. Application Only Access
- C. Database Security
- D. Program Security
- E. Security for Other Application Objects

VIII. Network Security and Logging
- A. Client Access Security
- B. TCP/IP and Host Server Security
- C. TELNET, FTP, ODBC, RMTCMD
- D. Using Network Server Exit Programs
- E. NetServer and IFS Shares

IX. Auditing Capabilities
- A. The Security Audit Journal
- B. Auditing Sensitive Files and Objects
- C. Auditing Powerful Users
- D. Auditing Command Usage
- E. Reporting from QAUDJRN
- F. Managing QAUDJRN Receivers

X. IBM i Navigator Security