www.400SCHOOL.COM

IBM i (iSeries, AS/400)
QAUDJRN Auditing and Forensic Analysis Workshop
(SC22)
2 Days(70% Lecture, 30% Lab/Exercises)

This Live Hands-On Workshop provides the student with an understanding of the IBM i Security Audit Journal (QAUDJRN) along with a comprehensive view of the auditing facilities available on the system.

Students will learn how to configure the system auditing facilities to audit the activity of Users, access to sensitive Objects and Security related events, like authority failures and invalid logon attempts.

In addition to learning how to audit these various activities, students will learn how to properly extract meaningful information from the QAUDJRN Security Audit journal to perform forensic analysis of audited events.

This workshop also provides the information needed to create and maintain the QAUDJRN Security Audit journal and associated journal receivers.

Prerequisites: Basic knowledge of IBM i (iSeries, AS/400) Security Concepts.

Course Outline

Introduction to QAUDJRN and Auditing
What is Security Auditing using QAUDJRN?
Determining the current QAUDJRN Setup
Creating the QAUDJRN Journal
Changing the Current QAUDJRN settings
High Availability Software Considerations

Maintaining QAUDJRN
Configuration of Journal Receivers
Determining Disk Space Requirements
Creating and Deleting Journal Receivers
Policy for Retention of Journal Receivers
Backup of Journal Receivers
Aging the Journal Receivers

Major Configuration Options for Auditing
QAUDCTL System Value Settings
QAUDLVL System Value Settings
QCRTOBJAUD System Value Settings
Other Auditing System Values
CRTOBJAUD Library Settings
OBJAUD Object and User Settings
AUDLVL User Setting

Configuring Auditing of Security Events
Determining/Configuring what is Audited
Auditing at the System Level
Auditing at the User Level

Configuring User Auditing
Determining/Configuring what is Audited
Auditing User Activity
Auditing a User's CL Commands
Auditing Access to a User Profile

Configuring Object Auditing
Determining/Configuring what is Audited
Auditing Access to Sensitive Files
Auditing the Use of Sensitive CL Commands
Auditing Access to other Objects
High Availability Software Considerations

Extracting Information from QAUDJRN
Determining the Availability of Audit Data
Various Extraction/Reporting IBM commands
Pros and Cons of Extraction Methods
Using the CPYAUDJRNE Command
Alternate methods for Advanced Filtering

Reporting Extraction Results
Extraction File Formats (QASYxxJ5)
Using the J5 Journal Entry Formats
Using RUNQRY/WRKQRY Commands
Download to MS/Excel
Using SQL
Other Reporting Tools

Forensic Analysis Scenarios/Examples
What CL Commands were run by a User?
Who used a Sensitive CL command?
Who Changed that System Value?
What new objects were created?
Who deleted that file?
Who looked at that sensitive file?
What files were opened for ODBC?
What files were accessed using FTP?
Where do the bad logons come from?
Who tried to access information they were not authorized to?
Other Scenarios/Examples as requested

For more information, call (314) 932-2430 or (800) 936-3140
Or e-mail info@400School.com

The 400 School, Inc – 1828 Canyon View Ct. – St. Louis, MO 63017