Course Outline

IBM i (iSeries, AS/400) QAUDJRN Auditing and Forensic Analysis Workshop

Course Summary

Description

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.

Topics

- Introduction to QAUDJRN and Auditing
- Maintaining QAUDJRN
- Major Configuration Options for Auditing
- Configuring Auditing of Security Events
- Configuring User Auditing
- Configuring Object Auditing
- Extracting Information from QAUDJRN
- Reporting Extraction Results
- Forensic Analysis Scenarios/Examples

Audience

This course is designed for those wanting to gain an understanding of the IBM i Security Audit Journal (QAUDJRN) and the auditing facilities available on the system.

Prerequisites

Before taking this course, you should have basic knowledge of IBM i (iSeries, AS/400) Security Concepts.

Duration

Two days

Course Outline

IBM i (iSeries, AS/400) QAUDJRN Auditing and Forensic Analysis Workshop

Course Outline

I. Introduction to QAUDJRN and Auditing
- A. What is Security Auditing using QAUDJRN?
- B. Determining the current QAUDJRN Setup
- C. Creating the QAUDJRN Journal
- D. Changing the Current QAUDJRN settings
- E. High Availability Software Considerations

II. Maintaining QAUDJRN
- A. Configuration of Journal Receivers
- B. Determining Disk Space Requirements
- C. Creating and Deleting Journal Receivers
- D. Policy for Retention of Journal Receivers
- E. Backup of Journal Receivers
- F. Aging the Journal Receivers

III. Major Configuration Options for Auditing
- A. QAUDCTL System Value Settings
- B. QAUDLVL System Value Settings
- C. QCRTOBJAUD System Value Settings
- D. Other Auditing System Values
- E. CRTOBJAUD Library Settings
- F. OBJAUD Object and User Settings
- G. AUDLVL User Setting

IV. Configuring Auditing of Security Events
- A. Determining/Configuring what is Audited
- B. Auditing at the System Level
- C. Auditing at the User Level

V. Configuring User Auditing
- A. Determining/Configuring what is Audited
- B. Auditing User Activity
- C. Auditing a User's CL Commands
- D. Auditing Access to a User Profile

VI. Configuring Object Auditing
- A. Determining/Configuring what is Audited
- B. Auditing Access to Sensitive Files
- C. Auditing the Use of Sensitive CL Commands
- D. Auditing Access to other Objects
- E. High Availability Software Considerations

VII. Extracting Information from QAUDJRN
- A. Determining the Availability of Audit Data
- B. Various Extraction/Reporting IBM commands
- C. Pros and Cons of Extraction Methods
- D. Using the CPYAUDJRNE Command
- E. Alternate methods for Advanced Filtering

VIII. Reporting Extraction Results
- A. Extraction File Formats (QASYxxJ5)
- B. Using the J5 Journal Entry Formats
- C. Using RUNQRY/WRKQRY Commands
- D. Download to MS/Excel
- E. Using SQL
- F. Other Reporting Tools

IX. Forensic Analysis Scenarios/Examples
- A. What CL Commands were run by a User?
- B. Who used a Sensitive CL command?
- C. Who Changed that System Value?
- D. What new objects were created?
- E. Who deleted that file?
- F. Who looked at that sensitive file?
- G. What files were opened for ODBC?
- H. What files were accessed using FTP?
- I. Where do the bad logons come from?
- J. Who tried to access information they were not authorized to?
- K. Other Scenarios/Examples as requested