System i (AS/400) Security and Compliance Assessment for the IT Auditor

Course Summary

Description

This Hands-On Workshop provides a guided walk-through of a Security and Compliance Assessment performed on the IBM System i(AS/400, iSeries. Students will learn the assessment methodology and techniques used by leading Security Experts.

Workshop materials include the Class Student Guide, along with model Assessment Checklists and numerous Security assessment reference documents

Objectives
At the end of this course, students will be able to:

- Perform security assessments
- Understand the risks associated with vulnerabilities that are discovered during the assessment process

Topics

- System i Assessment Overview
- Assessing System Level Security
- Assessing User Profiles
- Use of Adopted Authority
- Object Oriented Architecture
- Using the Security Toolkit for Reporting
- Work Management Security
- Evaluating Application Security
- Evaluating Network Security
- Using System Auditing Capabilities
- Using the IBM System i Navigator GUI

Audience

The workshop is designed specifically for those that perform IT audits and risk and vulnerability assessments on this popular IBM platform.

Prerequisites

Students should have basic knowledge of IT Security concepts.

Duration

Three days

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

ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

System i (AS/400) Security and Compliance Assessment for the IT Auditor

Course Outline

I. System i Assessment Overview
- A. The Assessment Process Overview
- B. Auditor User Account Requirements
- C. Generating and Accessing Reports
- D. Importing reports into Excel and Word

II. Assessing System Level Security
- A. Evaluating Security System Values
- B. Other Important System Values to Inspect
- C. Review SST Access, SST Users/PWD
- D. Review QSECOFR Account Access
- E. Review 3rd Party Tool Software

III. Assessing User Profiles
- A. Importing User Information into Excel
- B. Understanding User Profile Properties
- C. Password Rules and Restrictions
- D. Identifying Dormant User Accounts
- E. Special Authority Assignment
- F. Limited Capabilities Usage
- G. Usage of Group Profiles
- H. Examine possibility of User Profile Hijacking
- I. Examine User Initial Programs
- J. Common mistakes in User Profiles

IV. Use of Adopted Authority
- A. Understanding Adopted Authority
- B. Finding Adopting Back-Door Programs

V. Object Oriented Architecture
- A. Identify In-Scope Libraries and Directories
- B. Evaluate Library and Object Authorities
- C. Evaluate IFS Directory Authorities
- D. Review Object Ownership
- E. Understanding Private Authorities
- F. Understanding *PUBLIC Authority
- G. Examine the Use of Authorization Lists
- H. Common Authorization List Errors

VI. Using the Security Toolkit for Reporting
- A. Using SECTOOLS/SECBATCH Menus
- B. Security Jobs in the Job Scheduler

VII. Work Management Security
- A. Examine Sign-on Screen Vulnerabilities
- B. Checking for Library List Vulnerabilities
- C. Checking for Trojan Horse Programs
- D. Checking Job Description Vulnerabilities
- E. Examining Subsystem Entries

VIII. Evaluating Application Security
- A. Review Vendor supplied schemes
- B. Examine Database Security
- C. Reviewing files for Sensitive Data
- D. Examining the use of Database Journaling
- E. Examine Program Security
- F. Security for Other Application Objects
- G. Security of Sensitive Reports in OUTQs
- H. Checking the Status of Backups

IX. Evaluating Network Security
- A. DSPNETA to review System i Access Security
- B. TCP/IP and Host Server Security
- C. TELNET, FTP, ODBC, RMTCMD
- D. Review WRKFCNUSG
- E. Review NetServer Shares
- F. Review NETSTAT for Server Activity
- G. Evaluating the Exit Point Registry
- H. Checking DDM Security

X. Using System Auditing Capabilities
- A. The Security Audit Journal - QAUDJRN
- B. Auditing Access to Sensitive Files
- C. Auditing User Activity
- D. Auditing Security Related Events
- E. Reporting from QAUDJRN

XI. Using the IBM System i Navigator GUI

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