IBM i (iSeries, AS/400) Security Assessment

3 Days(70% Lecture, 30% Lab/Exercises)

This Workshop provides a guided walk-through of a Security Assessment performed on the IBM I (AS/400, iSeries). The workshop is designed specifically for those that perform IT audits and risk and vulnerability assessments on this popular IBM platform.

The class can be attended as a Lecture Only Student, or as a Hands-On Student Lab Student. Either option will be highly valuable to the student.

Students will learn an assessment methodology and techniques used by leading IBM i security experts. The instructor will guide the student through the in-depth assessment process, focusing on the student's own ability to perform security assessments, and understand the risks associated with vulnerabilities that are discovered during the assessment process.

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

Prerequisites: Basic knowledge of IT Security concepts.

Course Outline

Assessment Overview
The Assessment Process Overview
User Account Requirements
Generating and Accessing Reports
Importing reports into Excel and Word

Assessing System Level Security
Evaluating Security System Values
Review SST Access, SST Users/PWD
Review QSECOFR Account Access
Review 3rd Party Tool Software

Assessing User Profiles
Importing User Information into Excel
Understanding User Profile Properties
Password Rules and Restrictions
Identifying Dormant User Accounts
Special Authority Assignment
Limited Capabilities Usage
Usage of Group Profiles
Examine possibility of User Profile Hijacking
Common mistakes in User Profiles

Use of Adopted Authority
Understanding Adopted Authority
Finding Adopting Back-Door Programs

Object Oriented Architecture
Identify In-Scope Libraries and Directories
Evaluate Library and Object Authorities
Evaluate IFS Directory Authorities
Review Object Ownership
Understanding Private Authorities
Understanding *PUBLIC Authority
Examine the Use of Authorization Lists
Common Authorization List Errors

Using the Security Toolkit for Reporting
Using SECTOOLS/SECBATCH Menus

Work Management Security
Examine Sign-on Screen Vulnerabilities
Checking for Library List Vulnerabilities
Checking for Trojan Horse Programs

Evaluating Application Security
Review Vendor supplied schemes
Examine Library Security
Examine Database Security
Examining the use of Database Journaling
Examine Program Security
Security for Other Application Objects
Security of Sensitive Reports
Checking the Status of System Backups

Evaluating Network Security
DSPNETA to review IBM i Access Security
TCP/IP and Host Server Security
     TELNET, FTP, ODBC, RMTCMD
Review WRKFCNUSG
Review NetServer Shares and IFS
Using the NETSTAT command
Evaluating the Exit Point Registry

Using System Auditing Capabilities
The Security Audit Journal - QAUDJRN
Auditing Access to Sensitive Files
Auditing User Activity
Auditing the use of Sensitive Commands
Auditing Security Related Events
Reporting from QAUDJRN

Using the IBM System i Navigator GUI

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