

# **IBM i (iSeries, AS/400) Security Audit and Vulnerability Assessment Workshop (SC24)**

**4-Days (70% Lecture, 30% Lab/Exercises)**

This Live 4-Day Hands-On Workshop provides a guided walk-through of a Security Audit and Vulnerability Assessment performed on the IBM i (AS/400, iSeries). The workshop is designed for those that need to know how to detect security weaknesses and perform vulnerability assessments on the popular IBM i (iSeries, AS/400) platform.

Students will learn the assessment methodologies, techniques and the IBM supplied tools used by leading security experts. The workshop will guide the student through the in-depth assessment process, focusing on the student's own ability to properly assess security vulnerabilities, and understand the risks associated with vulnerabilities.

Workshop student materials include the workshop student guide, assessment checklists and numerous security assessment reference materials including the book "PowerTips for IBM i Security".

**Prerequisites: Basic knowledge of IT Security concepts.**

---

## **Course Outline**

### **System i Assessment Overview**

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

### **Assessing System Level Security**

Evaluating Security System Values  
Other Important System Values to Inspect  
Review SST Access, SST Users/PWD  
Review QSECOFR Account Access  
Review 3rd Party Tool Software

### **Assessing Security of User Accounts**

Extract and Reporting on Account Information  
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  
Examine User Initial Programs  
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  
Security Jobs in the IBM Job Scheduler

### **Work Management Security**

Examine Sign-on Screen Vulnerabilities  
Checking for Library List Vulnerabilities  
Checking for Trojan Horse Programs  
Checking Job Description Vulnerabilities

### **Evaluating Application Security**

Review Vendor Supplied Security Schemes  
Examine and Understand Database Security  
Examining the use of Database Journaling  
Examining 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  
Hidden Security Options of WRKFCNUSG  
Review NetServer Shares and the IFS  
Determining Network Servers in use  
Evaluating the Exit Point Registry  
Reviewing DDM Security

### **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 i Navigator for Windows**

---

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

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