Course Outline

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

Course Summary

Description

This live four-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".

Topics

- System i Assessment Overview
- Assessing System Level Security
- Assessing Security of User Accounts
- 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 i Navigator for Windows

Audience

This course 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.

Prerequisites

Before taking this course, you should have basic knowledge of IT security concepts.

Duration

Four days

Course Outline

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

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 Security of User Accounts
- A. Extract and Reporting on Account Information
- 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 IBM 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

VIII. Evaluating Application Security
- A. Review Vendor Supplied Security Schemes
- B. Examine and Understand Database Security
- C. Examining the use of Database Journaling
- D. Examining Program Security
- E. Security for Other Application Objects
- F. Security of Sensitive Reports
- G. Checking the Status of System Backups

IX. Evaluating Network Security
- A. DSPNETA to review IBM i Access Security
- B. TCP/IP and Host Server Security
  1. TELNET, FTP, ODBC, RMTCMD
- C. Hidden Security Options of WRKFCNUSG
- D. Review NetServer Shares and the IFS
- E. Determining Network Servers in use
- F. Evaluating the Exit Point Registry
- G. Reviewing 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 the use of Sensitive Commands
- E. Auditing Security Related Events
- F. Reporting from QAUDJRN

XI. Using the IBM i Navigator for Windows