System i (AS/400) Security Management Workshop

Course Summary

Description

This class provides a comprehensive treatment of System i (AS/400) security concepts along with practical instruction for implementing those concepts. Tips will be provided throughout the class on how to audit and detect faulty implementation that could compromise the system. Expanded hands-on lab exercises reinforce the concepts presented.

Topics

- System i Overview
- System Level Security
- All About User Profiles
- Object Oriented Architecture
- The Security Toolkit
- Work Management Security
- Application Security
- Network Security
- Auditing Capabilities
- Operations Navigator Security

Audience

This course is designed for those dealing with system setup and administration, including system administrators, security officers, and IT Auditors.

Prerequisites

Students should have some knowledge of basic computer security concepts.

Duration

Four 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

System i (AS/400) Security Management Workshop

Course Outline

I. System i Overview
- A. Menus, Commands
- B. Finding Commands
- C. OS Architecture

II. System Level Security
- A. Security System Values
- B. Security Levels
- C. Password Levels
- D. Protecting SST and DST services
- E. i/OS Encryption Options

III. All About User Profiles
- A. Working with User Profiles
- B. Special Authorities
- C. Limit Capabilities
- D. User Classes
- E. Group Profiles
- F. Reporting *Outfiles w/ Query/SQL
- G. Object Ownership
- H. Adopted Authority
- I. Finding Back-door Programs
- J. Preventing User Profile Hijacking
- K. Common mistakes in User Profiles

IV. Object Oriented Architecture
- A. A File is a File a Program is a Program
- B. Library and Object Authorities
- C. Security Commands for Objects
- D. Security Commands for IFS Objects
- E. Authority Shortcuts
- F. Authorization Lists
- G. Common Misunderstandings

V. The Security Toolkit
- A. SECTOOLS Menu Options
- B. Security Jobs in the Job Scheduler

VI. Work Management Security
- A. Sign-on Screen Vulnerabilities
- B. QSYSOPR Message Queue Authority
- C. Library List Vulnerabilities
- D. Checking for Trojan Horse Programs
- E. Job Description Vulnerabilities

VII. Application Security
- A. Vendor supplied schemes
- B. Application Only Access
- C. Database Security
- D. Program Security
- E. Security for Other Application Objects

VIII. Network Security
- A. Client Access Security
- B. TCP/IP and Host Server Security
- C. TELNET, FTP, ODBC, RMTCMD
- D. Using Network Server Exit Programs
- E. NetServer and IFS Shares
- F. Running the Intrusion Detection System

IX. Auditing Capabilities
- A. The Security Audit Journal
- B. Auditing Sensitive Files and Objects
- C. Auditing Powerful Users
- D. Auditing Command Usage
- E. Reporting from QAUDJRN
- F. Managing QAUDJRN Receivers

X. Operations Navigator Security

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