RSH CONSULTING

RACF - SECURING Z/OS UNIX

COURSE DESCRIPTION

This course is essential for anyone who intends to assume responsibility for maintaining z/OS Unix controls or wants to verify their z/OS Unix environment is properly secured and monitored. Participants will gain a solid understanding of z/OS Unix and how it can be secured in a system protected by RACF. The course will explore the assignment of user UID and group GID Unix identities and offer best practices for managing them. Powerful Daemon and Superuser authorities will be discussed along with guidance on their assignment and alternatives offered by UNIXPRIV profiles. Considerable time and attention will be devoted to file and directory access controls. Participants will learn how permission bits and Extended Access Control Lists (ACLs) grant access as well as how UNIXPRIV profiles influence access authorization. Techniques and best practices for granting permissions will be provided. The course includes descriptions and lab exercises for all commands used for administering permissions.

DURATION

5 Half-Day WebEx Sessions

WHO SHOULD ATTEND

- **RACF Administrators and Analysts** who want to take control of z/OS Unix security
- **IT Auditors** seeking to ensure regulatory compliance
- **Systems Programmers** who provide Unix and RACF technical support or implement system controls

WHAT YOU WILL LEARN

- Security-related z/OS Unix configuration options
- How z/OS Unix UIDs and GIDs are assigned
- Ways to grant full and limited Superuser authority
- Controlling Daemons and Servers
- How file and directory access is permitted
- Effective use of UNIXPRIV profiles
- Best practices for using permission bits and ACLs
- Ensuring security access events are logged
- Interpreting Unix-related ICH408I violation messages

PREREQUISITES

Completion of RSH's RACF Level II Administration plus six months of RACF work experience.

INSTRUCTOR - ROBERT S. HANSEL

Mr. Hansel has worked with RACF since 1986 as an administrator, auditor, consultant, and trainer. He is a prominent speaker on RACF audit and technical topics at conferences and user groups throughout the U.S.

COURSE OUTLINE

1. Introduction to z/OS Unix
   a. Overview, background, and functions
   b. OMVS Procedure and BPXPRMxx parameters
   c. Physical and Logical Unix File System
   d. Navigating the directory structure
   e. /etc Configuration Files
   f. Security Levels
2. Users and Groups
   a. Introduction to Unix UIDs and GIDs
   b. OMVS user and group profile segments
   c. User Security Packet (USP)
   d. Real, Effective, and Saved UID and GID
   e. Supplemental GIDs
   f. Replacing obsolete BPX.DEFAULT.USER
   g. Preventing duplicate UIDs and GIDs
   h. Automatic UID and GID assignments
   i. Surrogate authority
   j. FIELD class profiles
3. High Level Authorities
   a. Daemons
   b. Servers
   c. Superuser
   d. PRIVILEGED and TRUSTED Started Tasks
   e. FACILITY class BPX profiles and authorities
   f. UNIXPRIV class profiles and authorities
4. Program Controls and Attributes
   a. Maintaining a clean program environment
   b. Program profiles and libraries
   c. File extended attributes and authorities
5. File System Security
   a. FSACCESS and FSEXEC class permissions
   b. File system mount security options
   c. File Security Packet (FSP)
   d. RACF's role in file access authorization
   e. Owner, Group, and Other permission bits
   f. chown, chgrp, chmod, and umask commands
   g. setuid, setgid, and sticky-bit authorities
   h. Extended Access Control Lists (ACLs)
   i. setfacl and getfacl commands
   j. UNIXPRIV class profiles affecting authorization
   k. RESTRICTED user control
   l. Access authorization logic
6. Monitoring and Logging
   a. User auditing
   b. File and directory audit bits
   c. chaudit command
   d. UNIXPRIV profile auditing
   e. SETROPTS AUDIT and LOGOPTIONS settings
   f. Reporting tools - SMF unload and RACFICE
7. Other Control Issues
   a. IRRHFSU utility
   b. Identity Mapping - UNIXMAP and AIM
   c. Performance Tuning

To register for public courses or find out more about how RSH Consulting can help you better secure your system, call us at 617-969-9050, email us at info@rshconsulting.com, or visit our web site at www.rshconsulting.com.