Course Outline

AIX Systems Administration Security Issues v7.2

Course Summary

Description

This course will teach the commands and methods needed to setup and enforce a security domain on an IBM AIX system. The course will use a problem solving approach in the lab exercises to give systems administrator's hands-on reinforcement of these methods.

Objectives

After taking this course, students will be able to:

- Load the IBM AIX operating system with enhanced auditing features;
- Check file systems for security problems
- Design and enforce a secure password specification and modification mechanism
- Review security considerations in other areas of a UNIX system

Topics

- Advanced System Concepts for System Administrators
- System Security Features Updating
- Managing of System Users
- File System Security
- Using UNIX Log Files
- Network Security

Prerequisite

It is assumed that the student has completed the Fundamentals of AIX and the IBM AIX Systems Administration: Essential Operations courses, or has equivalent system experience.

Duration

One Day

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.

Course Outline

AIX Systems Administration Security Issues v7.2

Course Outline

I. ***Advanced System Concepts for System Administrators***
- A. Process concepts
- B. Shell command usage and review
- C. Overview of issues related to Unix security
- D. System administrator functions related to security

II. ***System Security Features Updating***
- A. Security levels in a UNIX system
- B. Rebuilding the UNIX kernel with auditing

III. ***Managing of System Users***
- A. Using the root account securely
- B. Password issues
- C. changing
- D. encryption
- E. aging and expirations
- F. shadow files
- G. Groups

IV. ***File System Security***
- A. File permissions review
- B. Special permissions: SUID,SGID,Sticky Bits
- C. Device files
- D. Using chown and chgrp
- E. Backups

V. ***Using UNIX Log Files***
- A. Users
- B. lastlog,utmp,wtmp,pacct,syslog
- C. System
- D. shutdownlog
- E. sulog/messages

VI. ***Network Security***
- A. Proper maintenance of the /etc/hosts file
- B. Using the "r" commands
- C. The restricted shell
- D. NFS security implications
- E. Known problems with SMTP (sendmail)
- F. Finger utility security issues
- G. TFTP issues

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.