

# Control & Security of UNIX

**COURSE DURATION:** 2-days

**CPE HOURS:** 16

**LEVEL:** Intermediate / Group-Live

**PREREQUISITES:** None

**ADVANCE PREPARATION:** None

The UNIX operating system is now standard in many organizations. Contrary to popular opinion, UNIX can be well secured as long as the available features are properly installed and maintained. This seminar will walk you through the UNIX operating system, describe the functions, control features and provide a step-by-step audit approach, complete with detailed audit programs and checklists. Many hardware suppliers have their own proprietary versions of UNIX. As these versions are based on System V or BSD UNIX, this seminar provides in depth coverage of both versions. You will receive detailed control checklists and an audit script to enable you to identify security weaknesses in UNIX. The instructor will demonstrate the audit script in the classroom to reinforce the concepts learned and show how easy it is to penetrate poorly secured UNIX platforms.

## WHO SHOULD ATTEND

This seminar is designed for internal auditors, UNIX administrators and security officers. Participants should be familiar with information security concepts, logical security and access controls.

## SEMINAR OUTLINE

### I UNDERSTANDING UNIX

- The UNIX World
- System V
- Berkeley Software
- Distribution

### II THE KERNEL

- Components and Functionality
- Configuration concerns
- Kernel change control
- BSD concerns
- AT&T concerns
- Audit program
- Control checklists

### III SYSTEM COMMAND DIRECTORIES

- Overview of the command directories
- System utilities (/bin)
- User utilities (/usr/bin)
- System configuration directory (/etc)
- System administration directory (/usr/lib)
- Other system libraries
  - /lib, /dev, /usr, /spool
- Security recommendations
  - BSD
  - AT&T
- Audit programs
- Control checklists

### IV UNIX FILESYSTEMS

- Types of files
- Inodes

- Directories
- Device files
- Sockets (BSD)
- Pipes (AT&T)
- Filesystem administration
- File permissions
- Security recommendations
- Audit programs, checklists

### V UNIX SHELLS

- Bourne shell, C shell
- Korn shell
- Shell interpreters

### VI THE SUPERUSER

- Overview
- Privileges, Functions
- File ownership
- Process ownership
- System administration
  - Installation
  - Adding and maintaining users
  - Maintenance
  - Backup and recovery
- Audit programs and control checklists

### VII DAEMONS AND PROCESSES

- Daemons
- Processes
- Audit programs, checklists

### VIII UNIX COMMUNICATIONS

- Understanding uucp
- Configuring uucp

- User file security and maintenance
- Important functions
- Log files
- Neighbor maintenance
- Security and control requirements
- Audit programs / checklists

### IX UNIX ACCOUNTING

- BSD accounting features
- AT&T accounting features
- Using accounting for security
- Charge back
- Resource planning
- Audit programs / checklists

### X UNIX SECURITY

- Setting up new accounts
- Account maintenance
- Controlling setuid
- Password control
- User and group profiles
- UNIX file and directory security

### XI THE AUDIT

- Audit preparation
- Audit scope and objectives
- Using the checklists
- Modifying the CANAUDIT audit programs