

# **Control and Security of UNIX**

|                              |                         |
|------------------------------|-------------------------|
| <b>Course Duration:</b>      | 2 Days                  |
| <b>CPE Hours:</b>            | 16 Hours                |
| <b>Level:</b>                | Intermediate/Group-Live |
| <b>Prerequisites:</b>        | None                    |
| <b>Advanced Preparation:</b> | None                    |

The UNIX operating system is common in many organizations. As with most operating systems, UNIX can be well secured as long as the available features are properly installed and maintained. This seminar will walk participants through the UNIX operating system, its functions and control features. 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. In order to identify security weaknesses in UNIX, participants will be provided with a step-by-step audit approach, detailed audit programs, control checklists and an audit script. 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 intended for Internal Auditors, UNIX Administrators and Security Officers. Participants should be familiar with information security concepts, logical security and access controls.

## **Seminar Outline:**

### **I) Introduction**

- Fundamentals
- UNIX history
- High-level review

### **II) Systems Overview**

- Physical security
- Users, passwords and authentication
- Users, groups and the super-user
- File system and security
- Daemons and processes
- Encryption

### **III) Network and Internet**

- Modem and dial-up security
- Local area networking
- Securing network services
- Network-based authentication
- Network file sharing

### **IV) Securing Your Systems**

- Patching
- Backups
- Accounts and access
- Integrity management
- System auditing, logging and forensics

### **V) Types of Attacks and Incident Procedures**

- Gaining remote access
- Local privilege escalation
- Denial-of-service attacks
- Trust relationships

### **VI) The Audit**

- Audit preparation
- Audit scope and objectives
- Using the checklists
- Modifying the Canaudit Audit Programs