CU006 - Unix Security for Users

Length: 1 Day

Description

This seminar is designed to make all users aware of the UNIX security vulnerabilities and show them how to prevent an unauthorized user from compromising their login account or data. The security features which are provided as part of the operating system are first discussed. Then, some of the ways in which unauthorized people may use to gain access to a UNIX system or another users files and directories are discussed. Next, the ways of preventing unauthorized access are described in detail, along with exact descriptions of each UNIX command and the way it is used. Each attendee will be provided with a self-assessment checklist and sample programs which will allow them to perform a personal audit on their account. The seminar concludes with a discussion of the actions a user should take if they suspect compromise of their login and/or files.

Course Objectives

Upon completion of this seminar the attendee will be able to:

1. state the security features of UNIX;
2. identify methods used to gain unauthorized access;
3. describe how unauthorized access can be prevented;
4. perform a self-audit on your login, files and directories;
5. state the actions to take if compromise is suspected.

Course Materials

1. UNIX Security for Users Student Guide and course notes.
2. User Security Checklist
3. Sample Audit Programs

Prerequisites

None

P.O. Box 307218
Columbus, Ohio 43230
+1 (866) 521-1776
http://www.corder.com

SAGE certification PREFERRED TRAINING PROVIDER

CU006 - Unix Security for Users

Course Content

I UNIX SECURITY CONCERNS

A Unauthorized Access by Trusted Users
B Unauthorized Access by Hackers

II UNIX SECURITY FEATURES

A Login
B Passwords
C File/Directory Access Permissions
   1. User
   2. Group
   3. Other
D umask
E Terminal Security
F Network Security

III METHODS USED TO GAIN UNAUTHORIZED ACCESS

A Loaned Out Logins
B Password Compromise
C File/Directory Permissions
D Tricking Authorized Users/System Administrators
E Problems in System Programs
F Intelligent Terminals

IV PROTECTING YOUR LOGIN, FILES, AND DIRECTORIES

A What to Look For
B User Responsibilities
   1. Setting Up The Environment (PATH)
   2. Changing File Access Permissions
   3. Changing File Ownership
   4. Changing File Group
   5. Checking File/Directory Access Permissions
   6. Last Login
   7. Auto Logoff
   8. Terminal Locking
   9. Data Encryption
C System Administrator Responsibilities
   1. Audits
   2. Access Modes
   3. Preventing Use of System Program Problems
D What to do if compromise is suspected

V COURSE CONCLUSION