Corder Enterprises International

Building World Class MIS Teams, for you!

CU005 - UNIX System Security

Length: 5 Days

Description

This course discusses UNIX security and how system managers and administrators can implement security measures on UNIX. The focus of the course is on the inherent security vulnerabilities commonly found on UNIX systems and how to correct them. Examples are presented which illustrate how to insure a high level of security confidence against unauthorized users from accessing the system. The common methods used to penetrate UNIX systems, gain unauthorized root access permission, become another user, plant trojan horses or spoofs, and other ways of circumventing the normal system protection are disclosed. Each attendee will receive detailed audit checklists and a diskette containing UNIX shell and C programs which will assist in performing security auditing and risk analysis.

Course Objectives

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

1. state the built-in UNIX security control mechanisms;
2. state the security venerabilities inherent to UNIX systems;
3. determine common methods used to gain unauthorized access to the system or data;
4. identify the bugs contained in UNIX system and application programs and how they are exploited by unauthorized users;
5. identify how trojan horses and spoofs are planted into the system and methods of detecting them;
6. state the minimum recommended file and directory access permissions;
7. perform a risk analysis and analyze the results; and
8. execute audit programs which will assist in maintaining system security.

Course Materials

1. UNIX System Security Student Guide and course notes.
2. Security Auditing Software Diskette (source code only).

Prerequisites

1. CU001 - Fundamentals of Unix
2. CU002 - Bourne Shell Programming or CU003 - Korn Shell Programming
3. Unix System Administration
4. A knowledge of shell and C programming is helpful.

CU005 - UNIX System Security

Course Content

I WHY UNIX SECURITY?

A UNIX Security Features
B UNIX Security Problems
C UNIX Security Levels
D The Trusted Computing Base
E The Orange Book

II USERS, PASSWORDS, GROUPS, AND THE SUPERUSER

A User Accounts
B Passwords
C Groups
D Substitute User
E User Security Checklist

III FILE SYSTEM SECURITY

A The UNIX File System
B Changing File Access Permissions
C Changing Owner and Group
D Set UID/Set GID
E Device Special Files
F Mountable File Systems
G File System Security Checklist

IV PROGRAMMING SECURITY

A Input and Output Functions
B Writing Secure Programs
C Compiling and Installing SUID/SGID Programs
D Programming As root
E Programming Security Checklist

V NETWORK SECURITY

A UUCP Security
B TCP/IP Network Security
C Network Security Checklist

CU005 - UNIX System Security

VI COMMON SECURITY PROBLEMS ON UNIX

- A System Problems
- B System Accounts Without Passwords
- C System Directories With Wrong Permissions
- D System Files with Wrong Permissions
- E Planting Trojan Horses
- F Spoofing Methods
- G Known Bugs, Trapdoors, and Viruses
- H Intelligent Terminals
- I Physical Access
- J Security Problem Checklist

VII PROTECTING YOUR SYSTEM

- A Security Administration
- B Security Compromises
- C Restricted Environments
- D Log Files
- E Recommendations for Securing Your System
- F Administrator Awareness
- G Auditing
- H What To Do If Your System Is Compromised
- I Using the Trusted Computing Base for Auditing
- J System Security Checklist

VIII COURSE CONCLUSION