775 route de l'aérodrome
ZA Agroparc
84000 Avignon
Tél 04 90 85 98 12
Fax 04 90 86 26 24
info@cit.fr
www.cit.fr

Linux – système sécurisé

Objectif : Toute personne souhaitant mettre en place une sécurité optimale sur un système Linux et plus particulièrement les administrateurs système et sécurité.

À l'issue de la formation, le stagiaire sera capable de :

- Savoir installer, administrer, faire évoluer une distribution

Prérequis : une bonne connaissance du système Unix/Linux est nécessaire

- 3 jours -

Introduction

- Le besoin, définition du D.I.C

Gestion utilisateur

- Rappels sur les notions de base de sécurité sur Unix: modes d'accès, comptes utilisateurs, groupes, utilisateurs génériques de gestion de ressources
- Fichiers /etc/passwd, /etc/group, /etc/shadow
- Gestion des groupes
- Vérification de cohérence : pwck
- Connexions du compte root, contrôle de connexions
- Connexions du compte root, contrôle de connexions
- Connexions du compte root, contrôle de connexions

Authentification

- Pam: gestion des modules d'authentification
- Principe de base, modification de fonctionnement
- Les modules : access, chroot, cracklib, env, ftp, groups, limits, listfile, mkhomedir, tally, time, unix, wheel

Sécurisation traitements

- Les risques : le déni de service, exemples de virus
- TP : exploitation d'un débordement de pile
- Les moyens de détection, la surveillance, les traces :syslog, l'accounting
- L'audit de securité

Sécurité du noyau

- Présentation de GrSecurity et SELinux. Installation, administration avec grAdm
- Mise en place des règles d'ACL. L'ACL GrSec
- Restrictions d'accès aux appels systèmes. Masquage de processus
- Visibilité du répertoire /proc. Restrictions chroot
- Introduction à UML (UserModeLinux) en mode SKAS

Les données

- Contrôle du système de fichiers : fsck
- Sauvegardes :Utilisation des sauvegardes pour la disponibilité des données
- Outils sauvegarde/archivage/compression : gzip, zip, tar, dd, cpio
- Création de CD ou disquettes de secours

Sécurité système de fichiers

- Sécurité: mise en place des contrôles d'accès (ACL)
- Quotas
- Options de montage: nosuid, nodev, noexec, ro

Déroulé de l'action

- **Type de stage**

  Session Inter-entreprises
  Session Intra

- **Horaires**

  9H00-12H30 /13H30-17H00

- **Méthode pédagogique**

  Alternance exposés théoriques
  et exercices pratiques

- **Suivi et assistance**

  Support de cours adapté au logiciel étudié et au niveau suivi
  Assistance téléphonique gratuite et illimitée

- **Validation des acquis**

  Exercice de validation en fin d'action