Linux - Système sécurisé

Référence : **LUUX117** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Une bonne connaissance du système Unix/Linux est nécessaire.

PROFIL DES STAGIAIRES

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

OBJECTIFS

• Savoir configurer les mécanismes de sécurité de Linux.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Linux

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

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