Phirio

Linux système sécurisé

UX117

Durée: 3 jours

Public :

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.

Connaissances préalables nécessaires :

Une bonne connaissance de l'administration des systèmes Unix/Linux est nécessaire.

Programme :

Introduction

Le besoin, définition du D.I.C.
Les attaques possibles.
Evaluation des risques.
Méthodes de protection.

Gestion utilisateurs

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. Codage des mots de passe. Création, modification, suppression de comptes utilisateurs.
Gestion des groupes :ajout, retrait d'utilisateurs, création d'administrateurs de groupes.
Affectation d'un mot de passe au groupe. Vérification de cohérence : pwck. Connexions du compte root, contrôle de connexions.
Outil de recherche de mots de passe.

Atelier : installation et mise en oeuvre de l'outil "John the ripper" en mode "single-crack".

Prise de privilèges : sudo, sudoers.

Authentification

pam: gestion des modules d'authentification. Présentation et exemples d'utilisation. Principe de base, configuration. Les modules : différents types de modules (auth, account, session, password).
Notion de pile de modules.

Atelier : mise en oeuvre de PAM et de quelques modules parmi les plus courants :access, chroot, cracklib, env, ftp, groups, limits, listfile, mkhomedir, tally, time, unix, wheel

Sécurisation traitements

Les risques : le déni de service, exemples de virus sur un système Linux.

Atelier : exploitation d'un débordement de pile. Les moyens de détection, la surveillance, les traces :

syslog, l'accounting. L'audit de securité. Méthodes de protection : démarche sur les systèmes Linux.

Sécurité du noyau

Les différentes approches de sécurisation du noyau.
Présentation de GrSecurity et SELinux. Travaux pratiques avec GrSecurity :installation, configuration du noyau, paramétrage du niveau de sécurité.
Administration avec grAdm2. Génération d'une politique : learning mode. 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. SELinux : principe, configuration du noyau, options du noyau.

Atelier : définition d'une politique de sécurité. Installation et activation de la politique de sécurité dans le fichier /etc/selinux/config.

Sécurité des données

Contrôle de la cohérence du système de fichiers : fsck. Procédure de vérification. Sauvegardes : définitions
Commandes et outils standards. Utilisation des sauvegardes pour la disponibilité des données. Outils sauvegarde/archivage/compression :
gzip, zip, tar, dump, restore, dd, cpio, rsync. Chiffrement des disques durs :mise en oeuvre de LUKS et dm-crypt
Protection de la mémoire :principe et outils de sécurisation.

Sécurité système de fichiers

Sécurité: mise en place des contrôles d'accès. ACL : principe des listes de contrôle d'accès POSIX.

Atelier : mise en place des ACL sur xfs. Les quotas : principe, mise en place dans le fichier /etc/fstab.

La commande edquota pour l'édition, et le paramétrage, et la commande quota pour la visualisation.

Atelier : mise en place des quotas