SECURISER UN SYSTEME LINUX (HARDENING)

OBJECTIFS

Sécuriser (bastionner) un serveur Linux sensible au niveau système et réseau. Sécuriser la séquence init et le bootloader. Apprendre à contrôler les accès au système. Savoir bloquer, journaliser et filtrer les accès. Mettre en œuvre des outils de détection des vulnérabilités.

RÉFÉRENCE

LINHA

PUBLIC VISÉ

Administrateurs systèmes

Administrateurs réseaux

PRÉ-REQUIS

Avoir suivi le cours Linux Administration (LINAD)

Maîtriser les points traités dans le cours Linux Administration (LINAD)

MÉTHODOLOGIE PÉDAGOGIQUE

50% d'apport théorique et 50% en exercices pratiques

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions et travail en groupe

DURÉE

2 journées de 7 heures

PLAN DE COURS

Identité

- Les utilisateurs et groupes sous Linux
- Focus sur le PAM (module d'authentification)
- Sudoers et classes d'utilisateurs

Les stratégies

- Sécurisation du bootloader
- Sécuriser la séquence init
- Savoir enlever les services et paquetages inutiles
- Rendre anonyme les bannières d'accueil de services
- Savoir renforcer les mots de passe : résistance et péremption
- Restreindre les privilèges administrateur
- Apprendre à contrôler les accès au système
- Contrôler finement les accès aux fichiers (ACL)
- Durcir les masques de permission sur les fichiers
- Bastion IPNetfilter / Iptable
- Détecter les ports réseaux à l'écoute
- Savoir bloquer, journaliser et filtrer les accès
- Savoir patcher et mettre à jour le système

Audit

- Evènements et journalisation système
- Savoir centraliser la journalisation
- Auditer les flux réseaux (tcpdump, wiresharck)
- Journalisation des communications réseaux (ntop)
- Savoir auditer l'intégrité des fichiers (tripwire)
- Auditer les accès au système de fichiers (utilisateurs et process)
- Mettre en œuvre des outils de détection des vulnérabilités
- Connaitre les techniques de sondes de détection d'intrusion

SUPPORT DE COURS

Un support de cours sera remis à chaque participant.

VALIDATION

A la fin de chaque journée, un questionnaire à choix multiple permet de vérifier l'acquisition correcte des compétences. Ce test reste disponible sur notre site web pour une consultation ultérieure

ATTESTATION

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.

DELIVRÉ EN

Inter-Entreprises

Intra-Entreprise