Formation Sécuriser un système Linux

Code : SEC-LINUX-100 Durée : 5 jours (35 heures)

Public visé

Responsables sécurité du SI, chefs de projets informatiques, administrateurs systèmes.

{{< formation-prerequis >}}

Objectifs pédagogiques

À l'issue de cette formation, vous serez capable de :

- Identifier les principales menaces de l'environnement Linux et les différentes solutions qui s'y rapportent
- Optimiser la sécurisation du système

Programme

Jour 1 - Matin

Introduction et généralités

- Généralités Linux, menaces/attaques, sécurité bonnes pratiques
- Audit initial système Linux

Jour 1 - Après-midi

Politiques de sécurité

- PSSI, standards ANSSI BP28
- Guide déploiement Linux (démarrage, noyaux, partitionnement, gestion logiciels)

Jour 2 - Matin

Identification et authentification

- Comptes, mots de passe, sudoers, PAM, centralisation SSSD

Jour 2 - Après-midi

Protection des fichiers

- Droits Unix, attributs étendus, ACL, capabilities, chiffrement, effacement

Jour 3 - Matin

MAC (Mandatory Access Control)

- SELinux

Jour 3 - Après-midi

Surveillance et sécurité réseau

- AIDE, Auditd, HIDS
- Sysctl, interfaces réseau

Jour 4 - Matin

Administration distante

- SSH
- DNSSEC

Jour 4 - Après-midi

PKI

- PKI clients Linux

Jour 5 - Matin

Filtrage

- Iptables, Nftables, Firewalld

Jour 5 - Après-midi

Audit final et architectures sécurisées

- Audit final, architectures sécurisées

Modalités d'évaluation des acquis

En cours de formation, par des études de cas ou des travaux pratiques. En fin de formation, par un questionnaire d'auto-évaluation.

{{< formation-require >}}

{{< formation-seealso >}}