SECURITE, SYSTEMES ET RESEAUX : INITIATION

OBJECTIFS

Mettre en œuvre les principaux moyens de sécurisation des systèmes et des réseaux. Comprendre et appréhender les différents types d'attaques (couche basse et applicatives). Comprendre les méthodes de cryptographie et d'authentification des utilisateurs. Sécuriser un système (hardening). Connaitre les outils et techniques à notre disposition en fonction du système.

RÉFÉRENCE

SECBA

PUBLIC VISÉ

Responsable sécurité,

Ingénieurs système et réseaux

Architecte sécurité,

Techniciens réseaux ou sécurité,

Administrateurs réseaux

PRÉ-REQUIS

Bonnes connaissances en réseaux et systèmes

MÉTHODOLOGIE PÉDAGOGIQUE

60% d'apport théorique et 40% 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

4 journées de 7 heures

PLAN DE COURS

Risques et menaces

- Etat des lieux de la sécurité informatique
- Attaques « couches basses »
- Attaques applicatives

Architectures de sécurité

- L'architecture en fonction des besoins
- Firewall
- Proxy serveur et relais applicatif

Sécurité des données

- Cryptographie
- Authentification de l'utilisateur
- Vers, virus, trojans, malwares et keyloggers

Sécurité des échanges

- Sécurité wifi
- IPSec
- SSL/TLS
- SSH

Sécuriser un système, le hardening

Audit et sécurité au quotidien

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