# LA SECURITE SOUS LINUX

## OBJECTIFS

Connaitre les concepts, méthodes et outils fondamentaux de la sécurité des réseaux et systèmes sous environnement Linux.

Savoir mettre en place des filtrages réseau et applicatif ainsi que des passerelles intranet-internet.

## RÉFÉRENCE

LINSE

## PUBLIC VISÉ

Administrateurs systèmes

Administrateurs réseaux

Architecte systèmes ou 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

4 journées de 7 heures

## PLAN DE COURS

**Sensibilisation à la sécurité du système d'information**

- Comprendre les enjeux, limites et compromis de la sécurité du SI
- Comprendre l'importance des composants humains et plans de secours
- Comprendre l'insécurité de TCP/IP et services réseaux Internet
- Comprendre les concepts d'intranet, extranet et Internet
- Comprendre l'insécurité des réseaux sans fil
- Les contre-mesures techniques classiques
- Chiffrement, authentification forte et contrôle d'accès
- Protection et intégrité des données, certificats
- Comprendre les systèmes cryptographiques et leurs applications
- Connaitre les garanties apportées par le chiffrement
- Authentification, intégrité et confidentialité
- Savoir créer des clés et des certificats de sécurité
- Mettre en place un chiffrement pour la communication et le transfert de fichiers
- Introduction aux infrastructures à clés publiques (PKI)

**Le filtrage réseau**

- Comprendre les différents types de filtrages réseau et contenu
- Savoir filtrer par service avec TCP wrappers et inetd
- Filtrer le réseau avec IP avec netfilter et iptables
- Mettre en place des règles de filtrage
- Le filtrage par inspection (stateful)
- Le filtrage en mode bastion
- Savoir utiliser des interfaces de configuration
- Traduction d'adresse (NAT) et redirection de port ou service
- Savoir réaliser une passerelle
- Le filtrage en mode pare-feu
- Savoir donner accès à des services accessibles depuis Internet
- Comprendre la notion de zone démilitarisée (DMZ)
- Savoir utiliser des ponts filtrants (bridges)

**Filtrage applicatif et VPN**

- Filtrer les contenus au niveau applicatif (proxy)
- Comprendre la notion de réseaux privés virtuels (VPN)

**Audit, détection d'intrusion et authentification**

- Tester les outils d'audit : nessus, ntop, nmap, wiresharck
- Mettre en œuvre des sondes de détection d'intrusion
- Connaitre les méthodes d'authentification sécurisée et centralisée

## 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