Formation Sécurité Linux

Durée : 3 jours
Public : Administrateurs systèmes confirmés
Pré-requis : Administration système et réseaux
Objectifs : Savoir sécuriser un serveur sous Linux
Référence : LIN40-F
Demandeurs d'emploi : Contactez-nous pour connaître les remises Pôle Emploi

Les différents niveaux de gestion de la sécurité

La sécurité au niveau du système d'exploitation
La sécurité au niveau des applications
La sécurité au niveau du réseau

Les droits au niveau de Linux

Rappels sur les permissions Unix standard
Extensions sur les systèmes de fichiers ext3/4
Fixer des autorisations sur des programmes (capabilities)
Nouvelles technologies : SELinux et AppArmor

Sécuriser les applications

L'authentification et l'environnement d'exécution avec PAM
Les technologies SSL/TLS
Espionnage et déchiffrage des données échangées
Le pare-feu applicatif TCP-Wrapper

Principe de fonctionnement de netfilter

Théorie : comment cela fonctionne ?
Les possibilités offertes
Mise en place dans le Noyau Linux
Contrôle des règles avec IpTable

Définition d'une DMZ d'hébergement

Mise en place pratique avec netfilter/iptables
Revue des options de sécurité du serveur Web Apache
Revue des options de sécurité du serveur de mail postfix
Revue des options de sécurité du serveur de noms bind
Transparence http

Définition du réseau local

Mise en place des accès interne/externe

Serveur Proxy cache web squid / squid guard
Installation, équilibrage de charge
Filtrage d'url squidguard

Accès externe aux machines

Les différents types de tunnels
Accès à distance sur une machine linux : ssh
VPN via le protocole GRE : pptpd
VPN avec IPSec

Détection d'intrusion et gestion des logs

Positionnement de la détection d'intrusion
Revue de Snort
Gestion de logs

Recherche de vulnérabilités

Les outils disponibles en Open Source
Présentation de NESSUS
Composants d'architecture
Formats des résultats

Maintenance

Gestion des backups
Réaction aux intrusions