FORMATIONS LINUX

MNIS – Tour de l'Horloge - 4, place louis Armand – 75012 Paris

TEL : 0950 070814

SRX

SECURISER UN SERVEUR SOUS LINUX

Durée : 4 jours

Prix : 1390€

GROUPE DE FORMATIONS

La formation fait partie du groupe de formation « Administration »

Administration		
LIN	Administration avancée	5
SRX	Sécurité sous Linux	4
VTX	Utiliser XEN sous Linux	4
VPI	IPSEC sous Linux	4

QUEL OBJECTIF

Ce stage très pratique vous montrera comment définir une stratégie de sécurité, sécuriser des serveurs Linux et maintenir un niveau de sécurité. Le cours prévoit entre autres la sécurisation du système isolé, la sécurisation du réseau dans l'entreprise ainsi que le nécessaire pour mener à bien un audit de sécurité.

PRE-REQUIS

Il est recommandé d'avoir une bonne connaissance de l'administration du système d'exploitation Linux.

POUR QUI

Cette formation est adaptée aux techniciens et ingénieurs, ayant besoin de sécuriser un serveur sous Linux.

POUR QUOI

Votre entreprise expose ses serveurs Linux à internet et vous devez minimiser les risques de compromission.

DEROULE DE LA FORMATION

INTRODUCTION

Pourquoi sécuriser un système ?
Terminologie DAC, MAC, RBAC
Définir une stratégie d'authentification sécurisée.
Les différents algorithmes de chiffrement. Chiffrement d'un mot de passe. Vérification d'un mot de passe.
La sécurité et l'Open Source
Exemple d'une vulnérabilité et solution de sécurisation.
L'installation de base: exemple Linux Debian, RedHat et les autres distributions.
Sécurisation du noyau et des drivers de périphériques.
Travaux pratiques Optimisation des installations dans une optique de gestion de la sécurité.

LA SECURITE LOCALE DU SYSTEME

Faible permissivité par défaut. Vérification des droits des fichiers, scripts et commandes efficaces pour diagnostiquer.
Systèmes de fichier en lecture seule, les attributs des systèmes de fichier.
Les outil d'analyse des logs. Réagir en temps réel, exemple de scripts.
Paramétrage de PAM dans les différents contextes.
Confinement de l'exécution des processus, rlimit, capabilities, chroot et jails.
Virtualisation et sécurité, la virtualisation comme outil de protection.
Cryptographie, utilisation de GPG pour chiffrer et signer.
Chiffrer une partition ou un disque. Détruire des données.
Travaux pratiques : Travail sur les droits, les PAM et les processus. Gestion de GPG.

LA SECURITE AU NIVEAU RESEAU

Architectures sécurisées. Serveurs sécurisés, DNS et mail.
IPSEC et les VPN
Mettre en place des filtres d'accès aux services.
Mise en place d'un firewall NetFilter sous Linux.
Le super-serveur xinetd. Les restrictions d'accès, mise en oeuvre de "pot de miel".
Réaliser un audit des services actifs. Le ssh.
Travaux pratiques : Configurer un Firewall et xinetd. Auditer les services fonctionnels.

LES UTILITAIRES D'AUDIT DE SECURITE

Les produits propriétaires et les alternatives libres.
Crack, John the Ripper, Qcrack.
Les systèmes de détection d'intrusion HIDS et NIDS.
Tester la vulnérabilité avec OpenVAS, nmap.
La mise en oeuvre d'un outil de sécurité.
Les outils de suivi de logs, syslogng
Travaux pratiques : Mise en oeuvre de quelques outils, OpenVAS, John, tripwire.