Formation Sécuriser un système Linux

La sécurité informatique est devenue une préoccupation essentielle des entreprises et donc des responsables informatique. La sécurisation de Linux est paradoxale : d'un côté, c'est un système qui peut être extrêmement hermétique et d'un autre côté, il est souvent très vulnérable compte tenu des nombreuses possibilités de configuration offertes. Cette formation permettra aux participants de découvrir l'ensemble des techniques de sécurisation d'un système Linux

Objectifs

- Comprendre comment bâtir une sécurité forte autour de Linux
- Savoir mettre en place la sécurité d'une application Linux
- Comprendre les fondamentaux de la sécurité informatique et notamment de la sécurité réseau
- Être capable de sécuriser les échanges réseaux en environnement hétérogène grâce à Linux

Public concerné

- Administrateurs systèmes et réseaux expérimentés

Prérequis

- Avoir suivi les formations Administration Linux niveau 1 - Installation et mise en oeuvre (XW302) et Administration Linux niveau 2 - Gestion et maintenance (XW303) ou connaissances équivalentes.

Une formation de 4 jours

Caractéristiques
Tarif : 2080 euros HT par personne
Numéro de formateur : 11754730575
Nombre d'heures : 28
Référence : XW305
Contact : Jean JUILLET
Telephone : 01.42.62.91.86
Email : contact@kaptive.com

Paris
03/03/2014
19/05/2014
15/09/2014
24/11/2014

Description des modules

Les enjeux de la sécurité

- Les attaques, les techniques des hackers
- Panorama des solutions
- La politique de sécurité

La cryptologie ou la science de base de la sécurité

- Les concepts de protocoles et d'algorithmes cryptographiques
- Les algorithmes symétriques et asymétriques (à clé publique), les fonctions de hachage
- La signature numérique, les certificats X-509, la notion de PKI

Les utilisateurs et les droits

- Rappels sur la gestion des utilisateurs et des droits, les ACLs
- La dangerosité des droits d'endossement
- La sécurité de connexion, le paquetage SHADOW

Les bibliothèques PAM

- L'architecture du système PAM, les fichiers de configuration
- L'étude des principaux modules

Le système SELinux ou la sécurité dans le noyau

- L'architecture du système SELinux
- Modifier les règles de comportement des exécutables

Les principaux protocoles cryptographiques en client/serveur

- SSH, le protocole et les commandes ssh
- SSL, l'utilisation de SSL et des certificats X-509 dans Apache et stunnel
- Kerberos et les applications kerbérorérisées

Les pare-feux

- Panorama des techniques pare-feux
- L'architecture Netfilter/Iptables, la notion de chaine, la syntaxe d'iptables
- La bibliothèque tcpd ou l'enveloppe de sécurité, la sécurisation via xinetd
- Mise en place d'un routeur filtrant, du masquerading et d'un bastion avec iptables
- Le proxy SQUID

Les VPN

- Panorama des techniques tunnels et VPN
- Le logiciel OpenVPN

La sécurisation des applications

- Principes généraux
- Sécurisation du Web, d'email, du DNS, du FTP

Les techniques d'audit

- L'audit des systèmes de fichiers avec AIDE et Tripwire
- Les outils d'attaque réseau
- La détection des attaques avec snort