

Formation Sécuriser un système Linux



La sécurité informatique est devenue une préoccupation essentielle des entreprises et donc des responsables informatiques. La sécurisation de Linux est paradoxale : d'un côté, c'est un système qui peut être extrêmement hermétique (à l'exception peut-être d'Unix BSD) et d'un autre côté, il est souvent très vulnérable compte tenu des nombreuses possibilités de configuration offertes

Objectifs

- Comprendre comment bâtir une sécurité forte autour de Linux
- Acquérir un niveau d'expertise plus élevé sur 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 expérimentés
- Administrateurs réseaux expérimentés

Pré requis

- Stage "L'essentiel pour administrer des serveurs Linux" (XW302) ou connaissances équivalentes.
- Stage "Maîtriser l'administration Linux" (XW303)

Une formation de 4 jours

Caractéristiques
Tarif : 2020 € HT par personne
Numéro de formateur : 11753687675
Nombre d'heures : 28
Référence : XW305
Contact : Patrick LE GOFF
Telephone : 01.76.60.66.10
Email : contact@kaptive.com

Paris
20/09/2010
29/11/2010

Description des modules

num	Module
1	Les enjeux de la sécurité
Détails	<ul style="list-style-type: none"> - Les attaques, les techniques des hackers - Panorama des solutions - La politique de sécurité ou l'épine dorsale de la stratégie de défense
2	La cryptologie ou la science de base de la sécurité
Détails	<ul style="list-style-type: none"> - 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
3	Les utilisateurs et les droits
Détails	<ul style="list-style-type: none"> - Rappels sur la gestion des utilisateurs et des droits, les ACLs - La dangerosité des droits d'endossement (SUID, SGID) - La sécurité de connexion, le paquetage SHADOW
4	Les bibliothèques PAM
Détails	<ul style="list-style-type: none"> - L'architecture du système PAM, les fichiers de configuration - L'étude des principaux modules
5	Le système SELinux ou la sécurité dans le noyau
Détails	<ul style="list-style-type: none"> - L'architecture du système SELinux - Modifier les règles de comportement des exécutable
6	Les principaux protocoles cryptographiques en client/serveur
Détails	<ul style="list-style-type: none"> - 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 kerbérorisées
7	Les pare-feux
Détails	<ul style="list-style-type: none"> - Panorama des techniques pare-feux : bastion, DMZ, routeur filtrant, proxy, masquerading - L'architecture Netfilter/Iptables, la notion de chaîne, 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
8	Les VPN
Détails	<ul style="list-style-type: none"> - Panorama des techniques tunnels et VPN - Le logiciel OpenVPN
9	La sécurisation des applications
Détails	<ul style="list-style-type: none"> - Principes généraux - Sécurisation du Web (Apache), du email (Sendmail, Postfix), du DNS (bind), du FTP
10	Les techniques d'audit
Détails	<ul style="list-style-type: none"> - L'audit des systèmes de fichiers avec AIDE et Tripwire - Les outils d'attaque réseau : le scanner nmap, le simulateur d'intrusion nessus - La détection des attaques avec snort, lire et écrire des règles snort