LINUX

Sécuriser un système Linux

4 jours (28h00) | LIN0004 | Num form : form-145 | Expertise

INFORMATIQUE / INFRASTRUCTURE / LINUX

À l'issue de ce stage vous serez capable de :

- 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

Niveau requis :

- Avoir suivi les formations "Linux administration"- Installation et mise en oeuvre" et "Linux administration" - Gestion et maintenance" ou connaissances équivalentes.

Public concerné :

- Administrateurs systèmes et réseaux expérimentés

Programme :

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 PARES-FEUX

- Panorama des techniques pares-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