LINUX - Sécurité

Référence : LNX-031

Durée : 4 jours

Le cours d'administration de la sécurité sous Linux permet d'acquérir les compétences d'administration système afin de gérer l'ensemble des problématiques sécurité au sein d'une entreprise.

Ce cours est basé sur une approche pratique agrémentée d'exercices sur des stations de travail. Il permet aux participants d'acquérir une expérience qui comprend la connaissance des risques actuels, leurs détournements et l'importance de la veille technologique.

Le stagiaire maîtrisera la sécurisation complète d'un parc de machines sous Linux.

Public & Pré-requis

Il s'adresse à des personnes ayant des connaissances d'administration système et qui souhaitent acquérir les compétences d'administrateurs Sécurité.

Une attention toute particulière sera apportée à la pédagogie du cours et à la compréhension des concepts présentés.

Pré-requis : connaissance de l'administration système Linux.

Sommaire

Introduction
La sécurité informatique – les attaques – la stratégie sécurité.

La cryptologie
Les algorithmes de chiffrement symétrique, à clé publique – signature – les protocoles – le chiffrement des systèmes de fichiers.

La sécurité locale
Sudo – la sécurité des utilisateurs – les mots de passes – les ACLs.

PAM

SELinux
Principe et mise en oeuvre – sécurité de type TE – MLS/MCS.

SSH
Protocole – les commandes – les clés – configuration avancée – port forwarding.

PKI et SSL
Certificat X509 – PKI – SSL – Stunnel.

Kerberos
Principe et mise en oeuvre – MIT – Heimdal – services «kerbérisés».

Les pare-feu
Principe – iptables – tcp_wrappers – xinetd – squid.

VPN
VPN – OpenVPN – IPSec.

Sécurisation des applications
Chroot - sécurisation des services, du réseau, d'Apache, du DNS, de MySQL et de l'email.

Audit
Attaques – tcpdump – wireshark – nmap – autres commandes et produits d'audit.

Sécuriser un serveur
Sécurisation d'un serveur – journaux de bord.