Formation Sécuriser un système Linux

Description de la formation Sécurité linux

Cette formation sécurité Linux vous montrera comment sécuriser des serveurs Linux au moyen d'outils et Logiciels Libres, ces outils sont nombreux, mûrs et adoptés par les principaux acteurs du marché.
À l'issue de cette formation, les participants sauront définir une stratégie de sécurité, sécuriser des serveurs Linux et maintenir un niveau de sécurité constant dans le temps.

Objectifs

Objectif opérationnel :

Sécuriser des serveurs Linux.

Objectifs pédagogiques :

- Sécuriser un système « isolé »
- Sécuriser un réseau dans l'entreprise
- Mener à bien un audit de sécurité

À qui s'adresse cette formation ?

Public :

Ce cours s'adresse aux administrateurs de serveurs et de réseaux ayant le souci de mettre en œuvre des serveurs sécurisés.

Pré requis :

La connaissance préalable de l'administration système Linux, des réseaux et protocoles TCP/IP sont nécessaires.

Contenu du cours Sécurité linux

Les enjeux de la sécurité Linux

Pourquoi sécuriser un système : De quoi doit-on se protéger, de qui, pourquoi peut-on être attaqué ?
Les attaques, les techniques des hackers
Panorama des solutions
La politique de sécurité ou l'épine dorsale de la stratégie de défense

Choisir une distribution dite « sécurisée »

Debian, RedHat et les autres distributions

Les utilisateurs, l'authentification

Définir une stratégie d'authentification sécurisée
Gestion des mots de passe, « éducation » des utilisateurs
Qui doit avoir un shell ?

Qui doit pouvoir se connecter ?
La notion de pseudo user

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

Vérification des droits des fichiers, scripts et commandes efficaces pour diagnostiquer

L'importance des droits sur les répertoires

Vérification automatisée : un changement de droit est il légitime ?

La dangerosité des droits d'endossement (SUID, SGID)

La sécurité de connexion, le paquetage SHADOW

Les bibliothèques PAM

L'architecture du système PAM

Les fichiers de configuration

Intérêt de restreindre les ressources du système au niveau PAM

Paramétrage des règles PAM (ulimit, hids, ...)

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,confinement de l'exécution des processus

Terminologie DAC, MAC, RBAC, contexte, modèle...

Définition de la politique de sécurité

Outils d'administration

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 : bastion, DMZ, routeur filtrant, proxy, masquerading

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 (OpenVPN)

Panorama des techniques tunnels et VPN

Le logiciel OpenVPN

La sécurisation des applications

Principes généraux

sécurisation du Web (Apache), du mail (Sendmail, Postfix), du DNS (bind), de FTP

Les techniques d'audit

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.