Sécuriser un système Linux/Unix

★★★★★

SII-299 **3 Jours (21 Heures)**

Description

Lors de ce stage pratique, vous apprendrez à définir une stratégie de sécurité, sécuriser des serveurs Linux et maintenir un niveau de sécurité optimal. La formation comprend des volets tels que la sécurisation du système isolé, la sécurisation du réseau dans l'entreprise et la conduite d'un audit de sécurité. Il s'agit d'une occasion d'acquérir des compétences pratiques indispensables pour assurer une sécurité renforcée des systèmes informatiques.

À qui s'adresse cette formation ?

Pour qui

Techniciens et administrateurs systèmes et réseaux.

Prérequis

Bonnes connaissances en administration des systèmes et réseaux.

Les objectifs de la formation

- Mesurer le niveau de sécurité de votre système Linux/Unix
- Connaître les solutions de sécurisation du système
- Savoir mettre en place la sécurité d'une application Linux/Unix
- Établir la sécurisation au niveau réseau

Programme de la formation

Introduction

- Sécuriser l'accès au domaine avec IPsec.
- Le firewall avancé de Windows 2008 Server.
- Configuration et administration du service RAS.
- Les VPN : principe du tunneling.
- Travaux pratiques Mise en oeuvre d'IPSec sous Windows.
- Paramétrage avancé du firewall.
- Mise en place d'un serveur RAS et d'un serveur RADIUS sous Windows 2008 Server.

La sécurité et l'Open Source

- Les corrections sont rapides, les bugs rendus publics.
- La technique d'approche d'un hacker : connaître les failles, savoir attaquer.
- Exemple d'une vulnérabilité et solution de sécurisation.
- Quelle solution ?

L'installation trop complète : exemple Linux

- Debian, RedHat et les autres distributions.
- Eviter le piège de l'installation facile.
- Allégement du noyau.
- Drivers de périphériques.
- Travaux pratiques Optimisation des installations dans une optique de gestion de la sécurité.

La sécurité locale du système

- Exemples de malveillance et d'inadvertance.
- Faible permissivité par défaut.
- Vérification des droits des fichiers, scripts et commandes efficaces pour diagnostiquer.
- FS en lecture seule : les attributs des fichiers, disponibilité et intérêt.
- Outils Tripwire.
- Conservation des logs, combien de temps ? L'outil d'analyse des logs : logwatch.
- Réagir en temps réel : exemple de script.
- Utiliser RPM comme HIDS.
- Paramétrage de PAM dans les différents contextes.
- Confinement de l'exécution des processus.
- Terminologie DAC, MAC, RBAC, contexte, modèle.
- Travaux pratiques Travail sur les droits, les logs et les processus.

La sécurité au niveau réseau

- Utiliser un firewall ? Utiliser les wrappers ? Mettre en place des filtres d'accès aux services.
- Configurer un firewall de manière sécurisée.
- Les commandes de diagnostic.
- Mise en place d'un firewall NetFilter sous Linux.
- Philosophie et syntaxe de iptables.
- Le super-serveur xinetd.
- Les restrictions d'accès par le wrapper, les fichiers de trace.
- Réaliser un audit des services actifs.
- Le ssh.
- Travaux pratiques Configurer un Firewall.
- Auditer les services fonctionnels.

Les utilitaires d'audit de sécurité

- Les produits propriétaires et les alternatives libres.
- Crack, John the Ripper, Qcrack.
- Les systèmes de détection d'intrusion HIDS et NIDS.
- Tester la vulnérabilité avec Nessus.
- La mise en oeuvre d'un outil de sécurité.
- Travaux pratiques Mise en oeuvre de quelques outils.