FORMATION : SÉCURITÉ

DS-102 : utiliser ACID avec un IDS *(1 jour)*

Logiciels utilisés

IDS Snort

Présentation

Les IDS sont les dernières innovations en matière de sécurité informatique. Elles permettent de détecter et d'enregistrer les attaques survenant sur le réseau. En « écoutant » de manière permanente le trafic échangé à un endroit clef de votre système d'information, cet équipement est capable de détecter les événements caractéristiques d'une attaque. L'IDS utilise un dictionnaire de signatures qui sont mises à jour régulièrement pour faire face aux nouvelles attaques.

Objectifs

Ce stage permet aux administrateurs Snort de déployer l'outil d'analyse ACID (Analysis Console for Intrusion Databases). Celui-ci permet une gestion centralisée de l'analyse des journaux Snort. Il produit également des rapports graphiques de l'activité des différents IDS déployés sur le Système d'Information.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Bonnes connaissances des réseaux TCP/IP

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Déploiement et administration de Snort (DS-101)

Programme

JOUR 1

Rappel sur l'IDS

Installation d'ACID
- Architecture IDS/base de données
- Pré-requis applicatifs
- Installation rapide LAMP (Apache, Mysql et PHP)

Configuration d'ACID
- Récupération et centralisation des données
- Intégration avec MySQL et Snort
- Contôles d'accès et sécurité

Modules additionnels
- Librairie GD pour tracer des graphiques

Le programme ci-dessus présente le programme initial de la formation DS-102 d'une durée d'une journée. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.