FORMATION : SÉCURITÉ

DS-101 : Déployer un IDS Snort *(2 jours)*

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 module permet à un administrateur de sécurité de découvrir le logiciel Snort ainsi que le module Acid (reporting). Le but est de savoir déployer la sonde sur un environnement de production et de pouvoir en retirer les informations pertinentes. Le stage met l'accent sur l'aspect pratique en proposant à chaque stagiaire de manipuler sa propre sonde.

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)

Programme

JOUR 1

Présentation du concept d'IDS

Intrusions, attaques et trafic suspect

Placer une sonde en mode passif
- Hub
- Port mirroring
- VLAN mirroring

Le logiciel libre Snort
- Historique
- Fonctionnalités
- Comparatif avec d'autres IDS

Maquette – Déployer Snort
- A partir de paquetages
- A partir des sources

JOUR 2

Configuration
- Modifier la configuration manuellement
- Administration via Webmin
- Les paramètres importants
- Le fichier de signatures
- Stockage des résultats
  - Fichiers
  - Base de données

Maintenir et exploiter la sonde
- Centraliser l'activité des sondes
- Mettre à jour et créer des signatures
- Comprendre les résultats
- Quelques outils d'aide à l'analyse
- Survol d'ACID (voir DS-102)

Le programme ci-dessus présente le programme initial de la formation DS-101 d'une durée de 2 jours. 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.