Fiche du cours

60 h

Titre :

SEC300 - Sécurité Systèmes & Réseaux

Description :

Ce cours forme les étudiants à la sécurisation des systèmes d'exploitation et des réseaux d'entreprise. Il couvre les bonnes pratiques de durcissement, la configuration de pare-feu, VPN et IDS/IPS, ainsi que la surveillance et la détection d'intrusions. Les participants apprennent à protéger les accès, sécuriser les flux et analyser les traces d'attaque pour réagir efficacement. Une attention particulière est portée aux environnements Linux/Windows et aux outils professionnels couramment utilisés.

Objectifs :

- Comprendre les bases de la sécurité système et réseau.*
- Mettre en place des mesures de durcissement et de filtrage réseau.*
- Détecter et analyser des comportements suspects.*
- Utiliser des outils d'inspection et de protection en environnement réel.

Chapitres :

1. Introduction à la sécurité système et réseau*
2. Durcissement des systèmes Linux et Windows*
3. Gestion des accès et authentification sécurisée (SSH, TLS/SSL)*
4. Pare-feu, VPN et segmentation réseau*
5. IDS/IPS : détection et prévention des intrusions*
6. Analyse réseau avec Wireshark et tcpdump*
7. Surveillance et journalisation centralisée*
8. Étude de cas pratique : mise en place d'une architecture sécurisée

À la fin :

Vous serez capable de sécuriser des systèmes et des réseaux d'entreprise, de déployer des pare-feu, IDS/IPS et VPN, d'analyser des flux réseau et d'identifier des tentatives d'attaque. Vous maîtriserez les bases opérationnelles nécessaires pour travailler au sein d'un SOC ou renforcer l'infrastructure défensive d'une organisation.