ID de Contribution: **8** Type: **Non spécifié**

Gérer une intrusion

mercredi 20 septembre 2006 16:30 (1h 30m)

Dans cette session, je propose d'aborder la gestion des conséquences dues à l'intrusion d'un pirate sur un système informatique d'un laboratoire, notamment comment s'y préparer et comment réagir face à un tel événement.
Nous aborderons les différents types d'incidents et attaques actuels mais aussi les symptomes d'une machine piratée, nous détaillerons les différents composants des systèmes et réseaux ayant un rôle actif dans le fonctionnement d'un système d'information en réseau, nous identifierons les informations pertinentes à rechercher parmi tous ces composants, puis nous verrons les bénéfices qu'apporte une administration réseau et système rigoureuse.
Nous présenterons différentes boites à outils utiles pour sauvegarder les informations pertinentes suite à une intrusion, nous décrirons le contenu des boites à outils et comment utiliser les principaux outils.
Un plan de préparation et d'action sera proposé. Ce plan détaillera les précautions et les recommandations à prendre en compte dans la sauvegarde des données.
Enfin, nous aborderons brièvement l'exploitation des données sauvegardées.

Auteur principal: PUGNERE, Denis (IPNL)

Orateur: PUGNERE, Denis (IPNL)

Classification de Session: Sécurité