Architectures réseaux sécurisées

ECTS
4 crédits

Volume horaire
54h

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

- Les principaux concepts associés à la conception et l'implémentation d'architectures réseaux sécurisées
- Les outils et techniques principaux permettant cette sécurisation et leur utilisation en fonction des différents contextes ainsi que des objectifs correspondants.
- Les vulnérabilités inhérentes aux architectures système et réseau et les grandes techniques d'intrusion ;
- Le fonctionnement des principales vulnérabilités du web.

L'étudiant devra être capable de :

- Distinguer les différents types de pare-feux ainsi que leurs capacités et limitations
- Définir et auditer une architecture de filtrage adaptée à un réseau informatique donné
- Choisir pour un tunnel IPsec les protocoles à utiliser, les modes de fonctionnement et un plan de routage adapté pour les passerelles associées
- Mettre en place et auditer un tel tunnel Ipsec
- Mettre en place ou auditer un VPN créé sur du IPsec manuellement ou en utilisant les outils tout-en-un du marché
- Mettre en place et auditer un système de détection d'intrusion éventuellement distribué avec des options de prévention
- Faire le design complet d'une architecture de sécurité pour un réseau complexe

- Identifier les limites et avantages de différentes solutions de détection d'intrusion ;
- Positionner les sondes de détection d'intrusion de manière efficace ;
- Analyse les évènements collectés par les sondes et corréler ces évènements pour identifier une menace réelle.
- Identifier les vulnérabilités dans les architectures web et proposer des solutions pour réaliser une protection efficace

Pré-requis nécéssaires

Une bonne connaissance des architectures Web, de la cryptographie et des réseaux.

Infos pratiques

Lieu(x)

Toulouse