Gestion de réseaux et sécurité
(56h)

Objectifs d'apprentissage

* Comprendre et mettre en oeuvre une solution de gestion de réseaux
* Appréhender les problèmes de sécurité affectant la sécurisation des systèmes d'information
* Avoir une vision d'ensemble des acteurs de la sécurisation (normalisation, clubs, cadre légal)
* Comprendre les principes de base de la sécurisation des réseaux et des services.

L'étudiant sera capable de :
* Concevoir, déployer et configurer une solution de gestion de réseaux adaptée aux besoins de l'environnement cible
* Interpréter et analyser une base d'informations de gestion (MIB)
* Expliquer les enjeux de la sécurité et décrire le rôle des différents organismes et des instituts de normalisation vis à vis de la sécurité
* Caractériser les éléments essentiels de base relatifs à la sécurisation des réseaux
* Analyser les attaques et intrusions et mettre en œuvre les mécanismes de protection nécessaires

Description synthétique des enseignements

Gestion des réseaux
* Problématiques de la gestion des réseaux
* Les aires fonctionnelles de la gestion : FCAPS (Fault, Configuration, Accounting, Performance, Security)
* Les modèles conceptuels de la gestion (fonctionnel, organisationnel, informationnel et protocolaire)
* Les standards SNMP et RMON de l'IETF
* Introduction à l'analyse de flux (NetFlow/IPFIX)
* Panorama des outils libres de supervision de réseaux

Sécurité
* Enjeux de la sécurité et propriétés - Approches pour la sécurisation
* Normes (ISO 15408, 27000,BS 7799...) ,
* Principes des méthodes d'analyse de risques - Rôles des organismes structurels (CERT, CLUSIF, CLUB 27001, ANSSI....)
* Techniques de sécurisation des réseaux (parefeux , protocoles sécurisés, PKI, tunneling...)
* Authentification - Kerberos
* Modèles de contrôle d'accès
* Analyse architecture DMZ - Analyse capacité de protection des pare-feux - Analyse attaques DoS TCP SYN et approches de protection - Intrusion detection system SNORT + SCAPY

Prérequis

* Fondements des réseaux TCP/IP

Références bibliographiques

* Network Management Fundamentals. A Clemm. CISCO Press. 2006
* SNMP MIB Handbook. L Walsh. Wyndham Press. 2008
* Sécurité informatique et Réseaux, Solange Ghernaouiti-Hélie - Eyrolles

Mots-clés

Gestion de réseaux - SNMP - NetFlow/IPFIX - Authentification - SSI - Analyse de risques - Attaques - Pare-feux - DMZ - PKI