Nom de l'UE : Bases théoriques de la sécurité	Semestre : S8

Objectifs de l'UE

Au terme de cette UE qui présente les modèles (outils et techniques)de sécurisation d'une architecture réseaux classique, l'étudiant saura :

- Identifier les différents types d'attaques ciblant les services déployés dans un réseau classique
- Sécuriser les services
- Concevoir et déployer une infrastructure de sécurité réseau classique
- Comprendre les standards cryptographiques et les utiliser pour déployer des solutions cryptographiques conformes à ces standards
- Appréhender les techniques de cryptage avancé

Description des ECUE

Modèles de sécurité

- Présentation générale des services (SMTP, WEB, FTP, Bases de données)
- Sécurisation des services
- Rapport entre la segmentation et l'architecture classique de sécurité d'un réseau classique (filaire et sans fil)
- Sécurité du réseau sans fil (IEEE802.11x/EAP/TLS/TTLS)
- Sécurité de l'architecture réseau classique (VPN, Firewall classique)

Cryptographie avancée

- Attaques et contre-mesures dans le chiffrement symétrique
- Attaques et contre-mesures dans le chiffrement asymétrique
- Méthodes cryptographiques avancées (chiffrement homomorphe, chiffrement fonctionnel, chiffrement basé sur les attributs, chiffrement basé sur l'identité, cryptographie à boîte blanche)

Pré-requis

Concepts de sécurité, Cryptographie, Services et protocoles réseaux

Bibliographie

S. Ghernaouti : Cybersécurité (5e édition, Sécurité informatique et réseaux), Dunod, 2016.