Nom de l'UE : Sécurité des systèmes et services réseaux	Semestre : S8

Objectifs de l'UE

Au terme de cette UE qui présente les concepts de sécurité des systèmes d'exploitation ainsi que ceux des services et protocoles réseaux, l'étudiant saura :

- Identifier les différents types d'attaques ciblant les systèmes d'exploitation des postes de travail et ceux des serveurs hébergeant les services déployés
- Identifier les différents types d'attaques ciblant les services et protocoles des couches OSI (Suite des protocoles TCP/IP)
- Identifier les outils et techniques de sécurité intégrant des fonctionnalités allant au-delà de la simple inspection du trafic réalisée par les pare-feux classiques
- Concevoir et déployer des infrastructures sécurité des architectures réseau complexes
- Identifier les propriétés de sécurité indispensables pour la protection des données manipulées par un poste de travail ou un serveur
- Identifier les risques et les vulnérabilités pouvant affecter un système d'exploitation
- Supprimer ou conserver les fonctionnalités d'un système d'exploitation en fonction de leur adéquation aux contraintes de sécurité
- Concevoir des mécanismes permettant de renforcer la sécurité d'un système d'exploitation

Description des ECUE

Sécurité des services et protocoles réseaux (Sécurité périmétrique)

- Attaques ciblant les couches 1 à 4 du modèle OSI
- Mesures contre les attaques des niveaux 1 à 4 (Firewall , IDS/IPS)
- Cas particulier des attaques par déni de services (DOS, Botnets et attaques DDOS)
- Attaques ciblant le DNS et contre mesure (DNSSEC, RPKI)
- Attaques ciblant les protocoles de routage (détournement des routes) et contre-mesures

Sécurité des systèmes d'exploitation

Sécurité Linux et Windows

- Attaques du noyau depuis l'espace utilisateur
- Mécanismes de protection de l'espace utilisateur
- Protection contre les attaques depuis l'espace utilisateur

Durcissement Linux

- Durcissement niveau 1 (pré-requis, gestion des droits, des services et des packages, Options FS, options kernel, durcissement des paramètres réseaux)
- Durcissement niveau 2 (gestion des droits, des utilisateurs et des packages)
- Durcissement niveau 3 (BIOS-séquence de boot, gestion des packages, implémentation de SELINUX)

Pré-requis
Concepts de sécurité, Services et protocoles réseaux, modèles de sécurité, systèmes d'exploitation
Bibliographie
S. Ghernaouti, Cybersécurité, Sécurité informatique et réseaux, Dunod, 5ème édition, 2016 G. Avoine, P. Junod, P. Oechslin et S. Pasinin, Sécurité informatique, Vuibert, 2015