Nom de l'UE : Gestion des menaces	Semestre : S9

Objectifs de l'UE

Cette UE présente les aspects inhérents à la supervision de la cybersécurité et aux tests d'intrusion, indispensables pour la sécurité prédictive et proactive d'un réseau complexe. A l'issue de ce cours, l'étudiant saura :

- Comprendre le fonctionnement des composants de l'infrastructure de sécurité d'un réseau complexe (Firewalls NextGen, NIDS, HIDS, Proxy)
- Concevoir et déployer une infrastructure de supervision de la cybersécurité d'un réseau complexe
- Concevoir et mettre en place des outils de collecte et d'analyse de logs
- Gérer et exploiter les indicateurs de sécurité
- Concevoir des règles de corrélation des événements et de détection d'attaques
- Concevoir des exploits,
- Exploiter les failles de sécurité dans différents environnements (réseaux filaires ou non, système d'exploitation, applications web, bases de données, …)

Description des ECUE

Détection et réponse aux incidents

- Concepts fondamentaux
- Découverte des ressources
- Collecte et analyse des log
- Tests d'intégrité des systèmes
- Création des règles de corrélation des événements et de détection d'attaques
- Indicateurs de sécurité, Dashboard
- Gestion des alertes

Outils et méthodologies de tests d'intrusion

- Vulnérabilités et attaques
- Techniques du pentesting,
- Pentesting réseau
- Pentesting des applications web
- Pentesting des réseaux sans fil

Pré-requis
Automates et langages, compilation, Concepts de la sécurité, services et protocoles réseaux, systèmes d'exploitation, sécurité des systèmes d'exploitation
Bibliographie