Module : Détection d'intrusions et gestion des alertes				Code	
				ING-4-SSIR-S9-P4	
Période	**Semestre 1**	*Volume horaire*	**21h**	*ECTS*	**2**

Responsable	**Rekhis Slim**	*email*	slim.rekhis@gmail.com
Equipe pédagogique	**Rekhis Slim** **Tounsi Mahmoud**		

1. Objectifs de Module *(Savoirs, aptitudes et compétences)*

L'objectif de ce cours est de comprendre les concepts et techniques utiles pour le déploiement des systèmes de détection d'intrusions. Le cours couvrira en détail les concepts fondamentaux liés aux intrusions et à la détection d'intrusions. Les étudiants apprendront à identifier les forces et les faiblesses de ces techniques/solutions et à les utiliser pour la mise en œuvre d'architectures sécurisées. À la fin de ce cours, l'étudiant sera capable de maîtriser les aspects techniques liés à la conception et à la mise en œuvre des solutions de prévention et de détection d'intrusions.

Compétences
C1.1 Maitriser et comprendre le fiche log
C1.2 Caractériser la différence entre les logs
C1.3 Interpréter la gestion des évènements log

2. Pré-requis *(autres UE et compétences indispensables pour suivre l'UE concernée)*

- Les commandes de base linux

3. Répartition d'Horaire de Module

Intitulé de l'élément d'enseignement	*Total*	*Cours*	*TD*	*Atelier*	*PR*
Module : Détection d'intrusions et gestion des alertes	21h	15h		6h	

4. Méthodes pédagogiques et moyens spécifiques au Module

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Supports de Cours
- Projecteur et Tableau
- Travaux dirigés

Bibliographie

Titre	Auteur(s)	Edition
Détection des intrusions dans les systèmes d'information : la nécessaire	Ludovic Mé	

prise en compte des caractéristiques du système surveillé		
Applied Network Security Monitoring: Collection, Detection, and Analysis	Applied Network Security Monitoring: Collection, Detection, and Analysis	

5. Contenu *(Descriptifs et plans des cours / Déroulement / Détail de l'évaluation de l'activité pratique)*	Durée allouée	
Détection d'intrusion et gestion des alertes		
Chapitre 1 : Concepts de base liés à la détection d'intrusion et aux systèmes de détection d'intrusion • Anatomie d'un scénario d'attaque et complexité de l'intrusion • Types d'intrusions • Objectifs et exigences de la détection d'intrusion • Modélisation des scénarios d'attaque • Défis pour la détection d'intrusion	Cours	3H
Chapitre 2 : Systèmes de détection d'intrusion réseau, hôte et application • Architectures IDS • Techniques de collecte de données NIDS, HIDS et AIDS • Déploiement des NIDS, HIDS et AIDS • Limites et forces de chaque type d'IDS • Interopérabilité des IDS	Cours Atelier	3H 3H
Chapitre 3 : Techniques de détection des scénarios : • Modèles et techniques de détection des abus • Modèles et techniques de détection des anomalies • Modèles et techniques de détection basés sur des spécifications • Analyse et discussion des modèles • Détection et prévention des intrusions sur le trafic chiffré	Cours Atelier	3H 3H
Chapitre 4 : Gestion des alertes • Correction des alertes/actions/scénarios • Corrélation horizontale et verticale	Cours	3H

• Fusion des alertes, vérification des alertes, normalisation des alertes, priorisation des alertes • Gestion des événements et des informations de sécurité		
Chapitre 5 : Attaques contre les IDS • Techniques d'évaluation des IDS • Sources d'ambiguïté dans la détection des intrusions • Attaques d'insertion, d'évasion et de déni de service (DoS) contre les IDS • Métriques d'évaluation de la détection des intrusions • Techniques d'évaluation des IDS et analyse ROC	Cours Atelier	3H 3H
TP 1 : Déploiement d'un IDS : Utilisation de Suricata	Cours Atelier	3H 3H
TP 2 : Déploiement d'un SIEM : Utilisation de Splunk	Cours	1.5H

6. Mode d'évaluation de Module *(nombre, types et pondération des contrôles)*

Eléments d'enseignement	Coeff	DS	EX	TP	PR
Module – Détection d'intrusion et gestion des alertes	1	40%	60%		

Pour valider le module, les étudiants passeront un examen dont le coefficient est de 60%, et un DS dont le coefficient est de 40%.
La durée de tous les examens (Examen, DS…) est de 1h30.

Quand à l'examen, il est planifié après l'écoulement des 7 semaines et portera sur toutes les thématiques enseignées tout au long des 21 heures.

Le module est validé si l'étudiant obtient une moyenne supérieure ou égal à 10 sur 20.