Module : Sécurité Informatique

Dernière mise à jour : 06/09/2022

Code	HE	HNE	ECTS
INFRES0001	21h	30h	2

Responsable Module	Imen Aouini
Enseignants – Intervenants	Equipe sécurité réseau
Unité pédagogique	UP Réseaux
Unité d'enseignement	Administration systèmes et réseaux
Pré-requis	Administration & sécurité des SE (Unix) Réseaux et protocoles TCP/IP Réseau IP et routage
Niveaux et Options	4ARCTIC, 4IoSyS, 4WIN, 4Gamix, 4NIDS, 4DS, 4Infini, 4ERP-BI, 4SIM, 4SLEAM, 4SAE, 4SE, 4TWIN.

Objectif du module :

A la fin de ce module l'apprenant sera capable de maîtriser les concepts fondamentaux de la sécurité informatique et de les mettre en pratique afin de concevoir des architectures sécurisées.

Mode d'évaluation :

La moyenne de ce module est calculée comme suit :

Note finale = Note de groupe (60%) + Note CC (40%)

Note de groupe : validation finale de projet

Note contrôle continu : suivi des workshops (40%)

Acquis d'apprentissage :

A la validation de ce module l'étudiant sera capable de :

	Acquis d'apprentissage	Niveau d'approfondissement (*)
AA1	Décrire les concepts de base de la sécurité Informatique (risque, méthodologie, et mécanismes)	1
AA2	Expliquer et manipuler les différents risques et attaques dans les réseaux informatiques	1&3
AA3	Expliquer et appliquer les concepts de la cryptographie (chiffrement, signature, certificat, SSL, etc)	2&3
AA4	Examiner une architecture réseau sécurisée (firewall, IDS, VPN, etc…)	4
AA5	Décrire et expliquer la sécurité des applications Web.	2

* : (1 : Mémoriser, 2 : Comprendre, 3 : Appliquer, 4 : Analyser, 5 : évaluer, 6 : Créer).

Contenu détaillé

Chapitre 1 : Notions de base de la sécurité informatique

- Expliquer notion de la sécurité informatique
- Identifier les objectifs de la sécurité
- Expliquer la terminologie de la sécurité
- Expliquer la méthodologie de sécurité
- Enumérer les règles de base de la sécurité informatique

Workshop : Préparation de l'environnement de travail et workshop analyse de vulnérabilités

Situation(s) d'apprentissage	Cours intégré
Durée	1h cours et 2h workshop
Rendu(s)	Rendu workshop

Chapitre 2 : Les principales attaques réseau

- Définir une attaque
- Identifier les différents objectifs d'attaques
- Classifier les attaques (actives/passives - internes/externes – directes/indirectes)

- Décrire les catégories des attaques (accès, modification, répudiation, saturation)
- Mettre en pratique les principales attaques réseau

Workshop : réalisation de quelques attaques réseaux

Outils : Linux Kali, metasploit, nmap, John the ripper, Wireshark, hping3, arpspoof

✔ Ex 1 : Attaque d'usurpation (ARP spoofing).

✔ Ex 2 : Attaque de Sniffing

✔ Ex 3 : L'attaque de reconnaissance

✔ Ex 4 : Attaque de déni de service (Synflooding).

Situation(s) d'apprentissage	Cours intégré
Durée	2cours et 2.30h TP
Rendu(s)	Rendu workshop

Chapitre 3 : Cryptographie

- Comprendre les besoins en cryptographie.
- Expliquer la terminologie de la cryptographie
- Expliquer les différents moyens cryptographiques :
  - Le chiffrement symétrique.
  - Le chiffrement asymétrique.
  - Le chiffrement hybride
  - Les fonctions de hachage
- Résumer le mécanisme de la signature numérique
- Expliquer le concept des certificats numériques
- Décrire le principe, l'architecture et le fonctionnement d'une PKI.
- Expliquer le principe de Secure Soket layer (SSL)

Whorkshop: Open SSL

✔ Chiffrement/déchiffrement (algorithme symétrique et asymétrique)

✔ Hachage et Signature numérique

✔ Création des certificats numérique

Situation(s) d'apprentissage	Cours intégré
Durée	2h et 2.30h TP
Rendu(s)	Rendu Workshop

++

Chapitre 4 : Architecture de sécurité Réseau

- Identifier les équipements de sécurisation d'un réseau informatique
- Comprendre la nécessité d'introduire des firewalls dans une architecture réseau
- Différents types de firewalls
- Différentes configurations de DMZ
- Définir le rôle et l'utilité d'un IDS/IPS
- Distinguer entre les techniques de détection d'intrusion : (par signature, Comportementale/Heuristique, par des règles)
- Introduire le réseau privé virtuel

Whorkshop :

PfSense : Installation - Création et modification de règles de firewalling

Situation(s) d'apprentissage	Cours intégré
Durée	1.30h et 1.30h TP
Rendu(s)	Rendu Workshop

Chapitre 5 : Sécurité des applications Web

- Identifier les menaces dans les applications web.
- Distinguer entres les classifications des vulnérabilités de sécurité dans les applications web. Top 10 Web Application Security Project (OWASP)
- Comprendre les principales attaques classifiées par OWASP.
- Comprendre les étapes de scan de vulnérabilité.

Workshop :

Thème : OWASP top 10 ; Utilisation du projet WebGoat,

Lab1: Attaque d'injection (SQL, Commande,…)

Lab2: Cross Site-Script (XSS)

Lab3: Cross Site Request Forgery (CSRF/XSRF)

Situation(s) d'apprentissage	Cours intégré
Durée	1h et 2h TP

Rendu(s)	Rendu Workshop

Validation du projet (par groupe)

- Exécuter un scénario de validation
- Répondre aux questions individuelles

Evaluation:

	Oral assessments	**Written exam/ MCQ**	**Report/ Homework**	**Presentation**	**TP**	**Project**
AA1		**X**	**X**			
AA2					**X**	
AA3					**X**	
AA4					**X**	
AA5					**X**	

Références :

Références bibliographiques :	**La cybersécurité, sécurité informatique et réseaux** Solange Ghernaouti (Ed DUNOD)