REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT
SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE
UNIVERSITE 8 MAI 1945
GUELMA
Faculté de Mathématiques,
D'Informatique et de Sciences de la Matière
Département : d'Informatique

وزارة التعليم العالـي
و البحث العلمـي
جامعـة 8 مـاي 1945
قالمـة
كليـة الرياضيـات، الإعـلام الآلـي
و علـوم المـادة
قسم: الإعلام الآلي

Année Universitaire 2020-2021

Syllabus – Sécurité Informatique

Nom du Syllabus :	**Sécurité Informatique**
Niveau :	3 LMD SI & ISIL
Année :	2020 - 2021
Semestre :	S6
Unité d'Enseignement :	UF3, Sécurité Informatique
Enseignant responsable :	Dr. Mohamed Amine Ferrag
Nb d'heures d'enseignement :	Cours : 1h30 + TD : 1h30
Nb d'heures de travail personnel pour l'étudiant :	2h
Nb de crédits :	5
Coefficient de la Matière :	3

OBJECTIFS:

Le module Sécurité Informatique fournit des bases solides dans l'ingénierie de la sécurité et permet aux étudiants de suivre facilement d'autres modules en sécurité et en cryptographie.

RESULTATS D'APPRENTISSAGE DES ETUDIANTS :

À la fin de ce cours, les étudiants seront capables de :

- Indiquer les concepts de base en matière de sécurité de l'information, y compris les politiques de sécurité, les modèles de sécurité et les mécanismes de sécurité.

- Expliquer les concepts liés à la cryptographie appliquée, y compris le texte en clair, le texte chiffré, les quatre techniques de crypto-analyse, la cryptographie symétrique, la cryptographie asymétrique, la signature numérique, le code d'authentification des messages, les fonctions hash et les modes de cryptage.

- Expliquer les concepts de code malveillant, y compris les virus, les chevaux de Troie et les vers. - Expliquer les vulnérabilités communes dans les programmes informatiques, y compris les vulnérabilités de débordement de tampon, le délai de vérification des défauts de temps d'utilisation, la médiation incomplète.

- Décrire les exigences et les mécanismes d'identification et d'authentification.

- Expliquez les problèmes d'authentification par mot de passe, y compris les attaques de dictionnaire (attaques de saisie de mot de passe), les stratégies de gestion de mot de passe et les mécanismes de mot de passe ponctuels.

- Décrire les menaces pour les réseaux et expliquer les techniques permettant d'assurer la sécurité du réseau, y compris le cryptage, l'authentification, les pare-feu et la détection d'intrusion.

PLAN DU COURS :

Chapitre 1 : Introduction à la sécurité informatique

1. L'architecture de sécurité OSI
2. Les services de sécurité
2.1. L'authentification
2.2. Le contrôle d'accès
2.3. La confidentialité des données
2.4. L'intégrité des données
2.5. La non répudiation
2.6. Le service de disponibilité
3. Les mécanismes de sécurité
4. Un modèle de sécurité réseau

Chapitre 2 : Les attaques informatiques

2.1. Définitions
2.2. Les types d'attaques
2.3. Les attaques réseaux
2.3.1. Les attaques contre le contrôle d'accès
2.3.2. Les attaques contre la confidentialité
2.3.3. Les attaques contre l'intégrité
2.3.4. Les attaques contre l'authentification
2.3.5. Les attaques contre la disponibilité
2.4. Tp : Installation et configuration du Snort sur Kali Linux

Chapitre 3 : Introduction à la cryptographie

3.1. Introduction
3.2. La cryptographie symétrique
3.2.1. Le chiffrement AES
3.3. La cryptographie asymétrique
3.3.1. Le chiffrement RSA
3.4. Les fonctions de hachage cryptographique
3.4.1. L'algorithme HMAC
3.4.2. L'algorithme MD5

Chapitre 4 : Les protocoles et les certificats de sécurité

4.1. Le protocole IPSec
4.1.1. IPSec Modes: Transport and Tunnel
4.1.2. En-tête d'authentification IPSec (AH)

4.1.3. IPSec Encapsulating Security Payload (ESP)
4.1.4. Echange de clés IPSec (IKE)
4.2. Le protocole Diameter
4.2.1. Structure du message de Diameter
4.2.2. Structure de l'AVP Diameter
4.2.3. Découverte des pairs dans Diameter
4.2.4. Établissement de connexion Diameter
4.2.5. Sécurisation des messages Diameter
4.3. Le protocole EAP
4.3.1. Les bases du protocole EAP
4.3.2. EAP dans les différentes versions de Windows
4.3.3. Configuration du protocole EAP
4.4. Le protocole SSL/TLS
4.4.1. Qu'est ce que SSL/TLS?
4.4.2. Les scénarios d'utilisation du TLS/SSL
4.4.3. Architecture TLS/SSL
4.4.4. Ports réseau utilisés par TLS / SSL
4.5. Le certificat numérique X.509

MODE D'EVALUATION : Examen final + Exposé

$$Note\ Finale = \frac{(Note\ TD * 40) + (Note\ Examen * 60)}{100}$$

BIBLIOGRAPHIE :

- Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.
- Kahate, A. (2013). *Cryptography and network security*. Tata McGraw-Hill Education.
- Ferrag, M. A & Ahmim, A. (2017). Security Solutions and Applied Cryptography in Smart Grid Communications. IGI Global, USA.
- Ferrag, M. A., Maglaras, L. A., Janicke, H., & Jiang, J. (2016). Authentication Protocols for Internet of Things: A Comprehensive Survey. *arXiv preprint arXiv:1612.07206*.
- Xiao, Y. (Ed.). (2016). *Security in sensor networks*. CRC Press.
- Li, Q., & Clark, G. (2013). Mobile security: a look ahead. *IEEE Security & Privacy*, *11*(1), 78-81.
- Ferrag, M. A., Maglaras, L., & Ahmim, A. (2017). Privacy-preserving schemes for ad hoc social networks: A survey. *IEEE Communications Surveys & Tutorials*, *19*(4), 3015-3045.