FICHE DESCRIPTIVE DE CERTIFICAT UNIVERSITAIRE

Intitulé CU

Sécurité des systèmes

Cadre 1

Diplôme principal concerné – Parcours concerné(s)

MASTER TIIR

Cadre 2

Autres diplômes concernés – Parcours concerné(s)

Cadre 3

Liens avec d'autres CU

CU Administration et virtualisation
CU Cryptographie appliquée
CU Comprendre et maîtriser les conteneurs logiciels avec Docker
CU Sécurité du réseau local
CU Analyse de risques/système de management de la sécurité de l'information

Cadre 4

Nombre d'heures / Nombre d'ECTS

C : 8 heures
TD : 12 heures
TP : 12 heures

Nb ECTS : 2

Modalités pédagogiques : Présentation des différents concepts, suivie de TP expérimentant le déploiement et l'administration sécurisés de systèmes/services.
Étude des systèmes, programmes comportant des failles (à partir de failles réelles ou d'un « cas d'école » fabriqué pour le besoin pédagogique).

Cadre 5

Université de Lille 1 SCIENCES ET TECHNOLOGIES

Niveau

Niveau (L/M/D) : Niveau I

Cadre 6

Pré-requis (connaissances et compétences)

Connaissances en programmation (C), du shell, de la structure d'un système (Unix).
Notions de réseau et de programmation Web, et de SQL.

Cadre 7

COMPETENCES EVALUEES

Compétences	**Evaluation**
Compétences disciplinaires : ▪ Connaissance des types de vulnérabilités, catégorisées par impact (fuite d'information, exécution de code, …), conditions d'exploitation (local, distant, pré-auth, …). Notion de « surface d'attaque ». ▪ Connaissance des causes de ces vulnérabilités : - Les composants sensibles d'un système typique, et fonctionnement de ces composants - Les problèmes liés au développement - Les problèmes liés au déploiement et à l'administration ▪ Bonnes pratiques de développement (programmation défensive, etc.) ▪ Identification (et limitation) des vecteurs d'attaques pour un système ▪ Automatisation des tâches liées à la sécurité (mise à jour, backup, etc.) ▪ Gestion correcte des droits d'accès et de l'authentification. ▪ Stratégies de mitigation : - Les méthodes de prévention d'exploitation (noyaux durcis, etc.) - Les méthodes d'isolation (virtualisation, etc.) - La détection d'intrusion (outils de surveillance, etc.) - La sécurité physique (chiffrement de disque, etc.) **Compétences Transversales :**	Examen théorique écrit, ainsi qu'une évaluation sur le travail réalisé lors des séances de TP.

Université de Lille 1 SCIENCES ET TECHNOLOGIES

Cadre 8

Compétences professionnelles :

- Avoir une vue d'ensemble des divers types de risques de sécurité qui peuvent impacter un système ou un programme.
- Savoir reconnaître les situations « à risque », c'est-à-dire savoir identifier les points « sensibles » d'un système ou d'un programme.
- Connaître les « bonnes pratiques » de développement et d'administration qui permettent d'éviter les failles de sécurité.
- Savoir déployer des stratégies de mitigation pour limiter l'impact d'une vulnérabilité

Secteurs d'activité

Secteurs d'activité : Informatique

Mots clefs des secteurs d'activité : sécurité informatique, cyber sécurité.

Cadre 9

Entreprises, branches professionnelles impliquées

Tous domaines confondus – fonctions traverses.

Cadre 10

Tarif FC

512 € (participant intégré au groupe formation initiale du Master)
2304 € (participant intégré à un groupe spécifique formation continue)

Cadre 11

Informations

Responsable du CU : Clément BALLABRIGA

Composante portant le CU : Faculté des Sciences et Technologies – Département d'INFORMATIQUE

Site web décrivant le CU (contenu, emploi du temps, mode pédagogique) : http://formation-continue.univ-lille1.fr/

Cadre 12