Sécurité des systèmes

UFR d'informatique, électronique, électrotechnique, automatique (IEEA)
Université de Lille – sciences et technologies

Université de Lille 1 SCIENCES ET TECHNOLOGIES

Formation continue

http://formation-continue.univ-lille1.fr

www.facebook.com/Formation.continue.Lille.1

OBJECTIFS

- 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

PUBLIC

Développeurs de programmes et administrateurs de systèmes informatiques

PRÉ-REQUIS

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

CONTENUS

PRÉSENTATION GÉNÉRALE 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 »

PRÉSENTATION 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

- 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.)

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)

CONTACT

SOPHIE RAMOS

03 20 43 32 24
sophie.ramos@univ-lille1.fr

Service formation continue
et alternance
Bâtiment B6
Cité scientifique
Rue Élisée Reclus
59655 Villeneuve d'Ascq Cedex

DURÉE - DATES

32 heures, 4 jours
8h30-12h30 14h-18h

11, 12, 14, 15 juin 2018

TARIF

2 304 €

LIEU DE LA FORMATION

Bâtiment M5
Salle TIIR, B03, aile B
Av. Paul Langevin
Cité scientifique
Villeneuve d'Ascq

RESPONSABLE PÉDAGOGIQUE

CLÉMENT BALLABRIGA
Maître de conférences
Département informatique, IEEA
Cité scientifique
Villeneuve d'Ascq