La formation continue à l'université

La force d'un réseau national

Formation qualifiante
Sécurité informatique – niveau 2

Public cible

Professionnel en activité ou demandeur d'emploi souhaitant se former ou renforcer ses compétences en sécurité informatique

Pré-requis

Etre titulaire d'un Bac+4 en informatique, ou avoir suivi le module de sécurité informatique de niveau 1

Durée

40 heures

Calendrier

Nous consulter

Lieu

Lens

Objectifs

A l'issue de la formation, vous serez capables de :

- Énoncer les concepts de base de la sécurité de l'information, les attaques informatiques et codes malveillants, les politiques et les modèles de sécurité, les mécanismes et outils de sécurité (outils préventifs comme les pare-feux, détectifs comme les IDSs et d'analyse post-mortem)
- Identifier les propriétés de sécurité (confidentialité, disponibilité, intégrité, etc.) violées par les attaques informatiques et les vulnérabilités pouvant aboutir à ces violations
- Expliquer et mettre en œuvre des concepts liés à la cryptographie (symétrique, asymétrique, signature numérique, fonctions de hachage, etc.). Mise en œuvre avec Openssl
- Auditer un système informatique (ex. réseau, application, base de données, etc.), analyser des logs et identifier des anomalies et des événements malveillants
- Utiliser et administrer des outils d'audit (ex. Wireshark, tcpdump) et de détection d'intrusions réseaux Snort

Contenu de la formation

- Introduction à la sécurité des programmes (principales attaques et menaces, tests, reviews de code, fuzzing, analyse statique, analyse dynamique, vérification, ...)
- Sécurité des programmes C (buffer overflow, interger overflow, tocttou, gestion dynamique de la mémoire, gestion d'erreurs, bonnes pratiques ...)
- Sécurité des programmes Java (modèle de sécurité Java : vérificateur de bytecode, chargeur de classes et contrôleur d'accès , bac-à-sable, politique de sécurité, API de sécurité JCA/JCE, JAAS, JSSE, bonnes pratiques...)
- Sécurité Web (principales technologies Web (PHP, ASP, JSP, CGI...) et leurs vulnérabilité, exemples d'attaques Web, outils de prévention et détection)

Tarif

Nous consulter

Candidature

Dossier de candidature à retirer auprès du service

Contenu de la formation (suite)

- Sécurité des réseaux :
  - Rappels de cryptographie, utilisation de gpg, ssh
  - Protocole SSL/TLS, programmation d'un client/serveur SSL/TLS
  - Pare-feux : filtrage de paquets (iptables/nft), proxy (squid)
  - VPN (utilisation d'OpenVPN, ipsec)
  - Kerberos : principe et protocole, utilisation de FreeIPA
  - SELinux

Recherche

La formation s'appuie sur le CRIL (Centre de Recherche en Informatique de Lens) unité mixte de recherche du CNRS et de l'université d'Artois (http://www.cril.univ-artois.fr).

Le CRIL regroupe une cinquantaine de membres et les recherches qui y sont développées concernent la conception de systèmes intelligents autonomes. En fonction des informations disponibles, de tels systèmes doivent être capables de prises de décision raisonnables afin d'atteindre au mieux leurs objectifs. Le CRIL structure ses activités selon deux axes principaux : d'une part, le traitement des informations imparfaites, dynamiques, contextuelles et multi-sources, et d'autre part, l'algorithmique pour l'inférence et la prise de décision. Les travaux conduits au CRIL trouvent des applications dans de nombreux domaines : transport, retail, génie logiciel, sécurité informatique, culture et patrimoine, …

Equipe pédagogique

L'équipe pédagogique est constituée d'enseignants-chercheurs et/ou chercheurs associés au CRIL renforcée par des professionnels partenaires issus d'ESN à rayonnement international comme régional (Atos Worldline, GFI, Capgemini, IBM, elosi, nelite, ...).

Cette formation est soutenue par le **Conseil Régional des Hauts-de-France.**

réalisation : service communication de l'université d'Artois - décembre 2018

FCU Artois
Faculté des Sciences
Rue Jean Souvraz - SP 18 - 62307 LENS CEDEX
Tél. 03 21 79 17 39
Mail : fcu-fare-lens@univ-artois.fr

www.univ-artois.fr