MINISTERE DE LA COMMUNAUTE FRANCAISE

ADMINISTRATION GENERALE DE L'ENSEIGNEMENT

ENSEIGNEMENT DE PROMOTION SOCIALE

DOSSIER PEDAGOGIQUE

UNITE D'ENSEIGNEMENT

FORMATION CONTINUE : INTRODUCTION A LA SECURITE DES SYSTEMES D'INFORMATION

ENSEIGNEMENT SUPERIEUR DE TYPE COURT
DOMAINE : SCIENCES

CODE : 7532 10 U32 D1

CODE DU DOMAINE DE FORMATION : 710
DOCUMENT DE REFERENCE INTER-RESEAUX

Approbation du Gouvernement de la Communauté française du
sur avis conforme du Conseil général

FORMATION CONTINUE : INTRODUCTION A LA SECURITE DES SYSTEMES D'INFORMATION

ENSEIGNEMENT SUPERIEUR DE TYPE COURT

1. FINALITÉS DE L'UNITÉ D'ENSEIGNEMENT

1.1. Finalités générales

Dans le respect de l'article 7 du décret du 16 avril 1991 organisant l'enseignement de promotion sociale de la Communauté française, cette unité de formation doit :

- concourir à l'épanouissement individuel en promouvant une meilleure insertion professionnelle, sociale, culturelle et scolaire ;
- répondre aux besoins et demandes en formation émanant des entreprises, des administrations, de l'enseignement et d'une manière générale des milieux socio-économiques et culturels.

1.2. Finalités particulières

L'unité d'enseignement vise à permettre à l'étudiant :

- ♦ d'interpréter les notions de base de sécurité des systèmes d'information et communication, et les différents types d'attaques ;
- ♦ d'identifier et d'expliquer la vulnérabilité d'un système d'information et de communication et de proposer les mécanismes de contrôle et d'authentification adéquats ;
- ♦ d'appliquer et d'informer sur les principes de sécurité des systèmes d'information et de communication ;

2. CAPACITES PREALABLES REQUISES

2.1. Capacités

En gestion et sécurisation des bases de réseaux

en disposant du matériel informatique nécessaire (routeur, switches, câbles informatiques, ordinateur serveur et ordinateurs clients éventuellement virtualisés, ...), de la documentation requise et d'un réseau,

face à un système informatique installé ou à installer, des consignes précises lui étant communiquées,

- ♦ de décrire les principales notions abordées ;
- ♦ de remédier à un dysfonctionnement simple (par ex : erreur d'adressage, câble débranché, …) ;

- de mettre en œuvre les procédures appropriées d'installation et de configuration d'un service déterminé ;
- de configurer le service sur le plan des fonctionnalités, afin de respecter les objectifs à atteindre ;
- d'identifier l'origine d'un problème rapporté par un utilisateur du système et de lui apporter une solution ;
- de justifier les choix réalisés.

En programmation orientée objet :

Pour atteindre le seuil de réussite l'étudiant sera capable d'effectuer l'analyse informatique, de programmer et de tester une/des applications techniques nécessitant l'emploi :

- des concepts de base de la programmation orientée objet (encapsulation, héritage, polymorphisme,…),
- d'une bibliothèque de classes pour l'accès à des bases de données relationnelles locales,
- de justifier les choix réalisés.

2.2. Titre pouvant en tenir lieu

Attestations de réussite des unités d'enseignement « BASES DES RESEAUX » code N° 2983 10 U31 D1 classée l'enseignement supérieur de type court **ET** l'unité d'enseignement « programmation orientée objet d'applications techniques » code N° 2982 23 U31 D1 classée l'enseignement supérieur de type court ;

OU

Attestations de réussite des unités d'enseignement « Administration, gestion et sécurisation des réseaux » code N° 7532 47 U32 D3 classée l'enseignement supérieur de type court, **ET** l'unité d'enseignement « programmation orientée objet » code N° 7525 21 U32 D2 classée l'enseignement supérieur de type court.

3. ACQUIS D'APPRENTISSAGE

Pour atteindre le seuil de réussite, l'étudiant sera capable,

En respectant les consignes liées à l'évaluation,
dans le respect du temps imparti,
sous la forme demandée et dans un local défini :

- d'expliquer différents concepts liés à la sécurisation des systèmes d'information et de communication ;

- d’identifier des outils et des technologies de sécurisation des systèmes d’information et de communication appropriés dans un scénario ou un contexte ;

Pour la détermination du degré de maîtrise, il sera tenu compte :

- du degré de clarté des propositions formulées,
- du degré de cohérence des propositions formulées,
- du degré de pertinence des propositions formulées,
- du degré de précision des propositions formulées,

4. PROGRAMME

L'étudiant sera capable :

- d'expliquer les paramètres de configuration de dispositifs et technologies réseaux usuelles (à titre d’exemple : pare-feu, routeur, switch, "load balancers, proxies, web security gateways, vpn concentrators, nids, nips, protocol analyzers, spam filter, utm security appliances, web application firewall, ...") ;
- d’expliquer les principes de sécurité fondamentaux en administration des réseaux (à titre d’exemple : "rule-based management, firewall rules, vlan management," configuration sécurisée des routeur, "access control lists", port security, 802.1x, flood guards, loop protection, implicity deny, network sepetation, log analysis, unitfied threat management, …) ;
- d'expliquer les rôles et conséquences des éléments d'architecture de réseau et des composantes de réseaux (à titre d’exemple : dmz, subnetting, vlan, nat, remote access, nac, virtualization, cloud computing, layered security, …) ;
- de sélectionner, en fonction d’un scénario donné, des protocoles et services réseaux usuels (à titre d’exemple : ipsec, snmp, ssh, dns, tls, ssl, tcp/ip, ftps, https, scp, icmp, ipv4, ipv6, iscsi, fiber, sftp, ftp, tftp, telnet, http, netbios, modèle OSI) et de pouvoir expliciter les rôles et les conséquences…) ;
- d’expliquer les rôles, vulnérabilités et vecteurs d'attaques courants des technologies liées aux systèmes de communication sans fil (à titre d’exemple : wpa, wpa2, wep, eap, peap, leap, mac filter, ssid broadcast, tkip, ccmp, placement d'antenne, contrôle de puissance d'émission, captive portals, monitoring de site, vpn, …) ;
- d’expliquer l'importance et les rôles des concepts associés à la notion de risque et de gestion du risque (à titre d’exemple : types de contrôles, faux positifs, faux négatifs, policies et réduction du risque, calcul du risque, approches quantitatives versus qualitative, vecteur de menace, threat likelihood, évitement, transfert, acceptation, mitigation et rejet du risque, …) ;
- d’expliquer les conséquences sécuritaires d'intégration des systèmes et des données avec des tiers (à titre d’exemple : convention d'interopérabilité, vie privée, conscience du risque, partage non autorisé, propriété des données, revue de convention et de conformité,…) ;

- d’expliquer les étapes et les besoins du déploiement de stratégies appropriées de mitigation du risque selon les scénarios les plus courants (à titre d’exemple : gestion du changement, gestion des incidents, revue des droits et des permissions des utilisateurs, audits régulier, application des policies, des procédures et mesures et technologies de contrôle, …) ;
- d’expliquer :
    - les procédures forensics de base ;
    - les procédures fondamentales de réponses aux incidents ;
    - l'importance des processus et stratégies de formation et de conscientisation à la sécurité ;
    - les mesures de contrôles physique et environnementaux ;
    - les "best practices" en gestion du risque (à titre d’exemple : business continuity concepts, fault tolerance, disaster recovery concepts, …) ;
    - les différents types de malware ;
    - les différents types d'attaques ;
    - les attaques d'ingénieries sociales, leurs impacts ainsi que leur cause et degré d'efficacité ;
    - les attaques sur les systèmes sans fil ;
    - les attaques sur les systèmes logiciels ;
    - les mécanismes et présenter les outils de découverte de vulnérabilités ;
    - l'importance, l'usage adéquat et les différences entre les tests d'intrusion et les analyse de vulnérabilités ;
    - l'importance, le rôle et les menaces mitigées par les mesures et techniques de contrôles applicatives ;
    - les concepts et technologies de sécurité liés aux technologies mobiles ;
- de sélectionner les mesures de contrôle approprié pour atteindre des objectifs de sécurité précis en fonction d'un scénario donné ;
- de sélectionner les mesures adéquates de mitigation et de déterrence en fonction d'un scénario donné ;
- de sélectionner les mesures adéquates de sécurités pour une machine hôte sur base d'un scénario donné ;
- d’expliquer les mesures de contrôle appropriées pour garantir la sécurité des données ;
- d’expliquer les méthodes disponibles pour mitiger les risques de sécurité dans les environnements statiques ;
- d’expliquer les fonctions et rôles des services d'authentification ;
- de sélectionner les mécanismes adéquats d'authentification, d'autorisation et de contrôle d'accès sur base d'un scénario donné ;
- d’expliquer et sélectionner les contrôles et techniques de sécurité adéquates associés à la gestion des comptes sur base des "best practices" ;
- de sélectionner et expliquer les concepts généraux de cryptographie sur base d'un scénario donné ;

- de sélectionner et expliquer les méthodes de cryptographie sur base d'un scénario donné ;
- de sélectionner et expliquer les mécanismes de PKI, gestion des certificats et technologies associées sur base d'un scénario donné ;
- Décrire les normes reconnues en sécurité (ISO 2700X, …).

5. CHARGE(S) DE COURS

Un enseignant ou un expert.

L'expert devra justifier de compétences issues d'une expérience professionnelle actualisée dans le domaine en relation avec le programme du présent dossier pédagogique.

6. CONSTITUTION DES GROUPES OU REGROUPEMENT

Aucune recommandation particulière

7. HORAIRE MINIMUM DE L'UNITE D'ENSEIGNEMENT

7.1. Dénomination du cours	**Classement**	**Code U**	**Nombre de périodes**
Techniques informatique et sécurité	CT	B	48
7.2. Part d'autonomie		P	12
Total des périodes			60
Nombre d'ECTS			**4**